VNNIC
Internet for all

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM INTERNET VIỆT NAM

HỆ THỐNG DNS

KIẾN TRÚC, QUẢN TRỊ, TỐI ƯU, ĐẢM BẢO AN TOÀN & ỨNG DỤNG CÔNG NGHỆ MỚI

iC PUBLISHER
NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM INTERNET VIỆT NAM

HỆ THỐNG DNS

KIẾN TRÚC, QUẢN TRỊ, TỐI ƯU, ĐẢM BẢO AN TOÀN & ỨNG DỤNG CÔNG NGHỆ MỚI

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

CHỈ ĐẠO BIÊN SOẠN

ÔNG NGUYỄN HỒNG THẮNG
Giám đốc, Trung tâm Internet Việt Nam

NHÓM BIÊN SOẠN

ÔNG NGUYỄN TRƯỜNG THÀNH
Trưởng phòng Kỹ thuật, Trung tâm Internet Việt Nam

ÔNG NGUYỄN VĂN TRÍ
Chuyên viên phòng Kỹ thuật, Trung tâm Internet Việt Nam

CHỊU TRÁCH NHIỆM XUẤT BẢN, NỘI DUNG

TS. TRẦN CHÍ ĐẠT
Giám đốc – Tổng biên tập

Chịu trách nhiệm bản thảo

BÀ NGÔ THỊ MỸ HẠNH
Phó Giám đốc – Phó Tổng Biên tập

Biên tập nội dung: **NGUYỄN LONG BIÊN**

Trình bày, thiết kế sách: **NGUYỄN NGỌC MẠNH**

Biên tập sách điện tử: **NGUYỄN TIẾN PHÁT**

Trình bày sách điện tử: **NGUYỄN THỊ THẢO**

NHÀ XUẤT BẢN THÔNG TIN VÀ TRUYỀN THÔNG

Trụ sở: Tầng 6, Tòa nhà Cục Tần số vô tuyến điện
115 Trần Duy Hưng, quận Cầu Giấy, TP. Hà Nội
ĐT Biên tập: 024.35772143; ĐT Phát hành: 024.35772138
E-mail: nxb.tttt@mst.gov.vn www.nxbthongtintruyenthong.vn; book365.vn; ebook365.vn; ebook.gov.vn
Số XNĐKXB: 2013-2025/CXBIPH/1-82/TTTT
Số QĐXB: 594/QĐ - NXB TTTT ngày 23 tháng 6 năm 2025
Mã ISBN: 978-604-45-1126-9
Nộp lưu chiểu Quý II năm 2025

MỤC LỤC

THUẬT NGỮ VÀ TỪ VIẾT TẮT **07**

DANH MỤC HÌNH VẼ **09**

LỜI NÓI ĐẦU **11**

PHẦN 1: QUẢN TRỊ VẬN HÀNH, TỐI ƯU HỆ THỐNG DNS **13**

I. Giới thiệu về DNS **14**

1. Khái niệm DNS 14

2. Vai trò và tầm quan trọng của DNS trong Internet 14

3. Lịch sử phát triển của DNS 15

II. Các khái niệm cơ bản **17**

1. Tên miền và địa chỉ IP 17

2. Cấu trúc phân cấp tên miền 17

3. Các thành phần của hệ thống tên miền 19

III. Quản lý, đăng ký tên miền, IP tại Việt Nam **23**

1. Quản lý, đăng ký tên miền 23

2. Quản lý, đăng ký sử dụng địa chỉ IP, số hiệu mạng 26

IV. Giao thức DNS **29**

1. Định dạng (Format) 29

2. Truyền tải (Transport) 33

V. Mô hình hoạt động của DNS **35**

1. Quá trình phân giải tên miền 35

2. Các loại truy vấn DNS 36

3. Mô hình Client-Server trong DNS 39

VI. Kiến trúc DNS **41**

1. Kiến trúc phân tán 41

2. Mô hình Master-Slave 41

3. Các loại máy chủ DNS 42

VII. Phân loại bản ghi DNS 44
1. Các bản ghi chính 44
2. Các bản ghi khác 49
VIII. DNS và IPv6 51
1. Ánh xạ tên miền và địa chỉ IPv6 51
2. Giao thức truyền tải trong mạng DNS IPv6 52
IX. Cài đặt và tối ưu DNS 54
1. Cài đặt máy chủ DNS 54
2. Tối ưu DNS 58
X. Các công cụ hỗ trợ quản lý, vận hành 62
1. Công cụ hỗ trợ cài đặt 62
2. Công cụ hỗ trợ giám sát, kiểm tra sức khoẻ 62
3. Công cụ hỗ trợ điều tra, truy vết (Troubleshooting) 65
4. Ghi nhật ký (Logging) 79

PHẦN 2: BẢO MẬT VÀ ỨNG DỤNG CÔNG NGHỆ MỚI 81
XI. Giải pháp DNS quy mô lớn, tăng cường tính sẵn sàng và chống chịu 82
1. Anycast là gì 82
2. Mối liên hệ giữa Anycast và DNS 83
3. Công nghệ và nguyên tắc hoạt động của DNS Anycast 84
4. Các mô hình triển khai DNS Anycast 84
5. Xu hướng phát triển DNS Anycast 86
XII. Bảo mật DNS 87
1. Các mối đe dọa đối với DNS 87
2. Một số dạng tấn công DNS phổ biến 87
3. DNS và Malware 93
4. Các biện pháp bảo mật 95
XIII. DNSSEC 113
1. Tổng quan về DNSSEC 113
2. Tính năng và ứng dụng của DNSSEC 117
3. Làm rõ những hiểu lầm về DNSSEC 118
4. Triển khai DNSSEC 118

XIV. DNS Abuse **120**
1. DNS Abuse là gì 120
2. Tác động ảnh hưởng của DNS Abuse 120
3. Giải pháp ngăn chặn, giảm thiểu DNS Abuse 121
XV. Các công nghệ mới trong DNS **122**
1. Các công nghệ mới trong DNS 122
2. DNS và 5G, IoT 123
3. DNS và CDN 128

PHẦN 3: CÁC BÀI THỰC HÀNH **135**
XVI. Thực hành (LAB) 136
1. Mô hình triển khai DNS tiêu chuẩn 136
2. Các bài thực hành 138

TÀI LIỆU THAM KHẢO **172**
1. Sách tham khảo 172
2. Danh sách các RFC chính 172

THUẬT NGỮ VÀ TỪ VIẾT TẮT

TỪ VIẾT TẮT	TÊN ĐẦY ĐỦ	MÔ TẢ
5G	Fifth Generation	Mạng di động thế hệ thứ 5
AI	Artificial Intelligence	Trí tuệ nhân tạo
APNIC	Asia Pacific Network Information Centre	Tổ chức quản lý tài nguyên Internet cho khu vực châu Á – Thái Bình Dương
AXFR	Full Zone Transfer	Đồng bộ toàn bộ zone tên miền
BGP	Border Gateway Protocol	Giao thức định tuyến động giữa các hệ thống mạng
BIND	Berkeley Internet Name Domain	Phần mềm mã nguồn mở sử dụng cho máy chủ DNS
ccTLD	Country Code Top-Level Domain	Tên miền cấp cao mã quốc gia (ccTLD)
CDN	Content Delivery Network	Mạng phân phối nội dung
DDNS	Dynamic Domain Name System	Hệ thống tên miền động
DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
DGA	Domain Generation Algorithm	Thuật toán tạo tên miền
DNS	Domain Name System	Hệ thống tên miền
DNSSEC	Domain Name System Security Exten-	Tiêu chuẩn an toàn mở rộng cho hệ thống DNS
Domain	Domain	Miền
DoH	DNS over HTTPS	Giao thức mã hóa các truy vấn DNS qua HTTPS
DoQ	DNS over QUIC	Giao thức mã hóa các truy vấn DNS sử dụng giao thức QUIC
DoT	DNS over TLS	Giao thức mã hóa các truy vấn DNS sử dụng Transport Layer Security (TLS)
eKYC	Electronic Know Your Customer	Định danh khách hàng điện tử
FQDN	Fully Qualified Domain Name	Tên miền đầy đủ
GDPR	General Data Protection Regulation	Quy định bảo vệ dữ liệu cá nhân của Liên minh Châu Âu
gTLD	Generic Top-Level Domain	Tên miền cấp cao dùng chung
HTTP	HyperText Transfer Protocol	Giao thức truyền tải văn bản (web) qua Internet
HTTPS	HyperText Transfer Protocol Secure	Giao thức truyền tải văn bản (web) mã hóa qua Internet
IANA	Internet Assigned Numbers Authority	Cơ quan quản lý và phân bổ số hiệu Internet
ICANN	Internet Corporation for Assigned Names and Numbers	Tổ chức quản lý tên miền và tài nguyên IP toàn cầu
IDC	Internet Data Center	Trung tâm dữ liệu Internet
IDN	Internationalized Domain Name	Tên miền đa ngữ
IETF	Internet Engineering Task Force	Tổ chức chịu trách nhiệm phát triển và thúc đẩy các tiêu chuẩn Internet

TỪ VIẾT TẮT	TÊN ĐẦY ĐỦ	MÔ TẢ
IoT	Internet of Things	Internet vạn vật
IPv4	Internet Protocol version 4	Giao thức Internet phiên bản 4
IPv6	Internet Protocol version 6	Giao thức Internet phiên bản 6
ISP	Internet Service Provider	Doanh nghiệp cung cấp dịch vụ Internet
IX	Internet Exchange	Trạm trung chuyển Internet
IXFR	Incremental Zone Transfer	Đồng bộ zone tên miền theo từng thay đổi
KSK	Key Signing Key	Khóa ký khóa sử dụng trong DNSSEC
ML	Machine Learning	Học máy
New gTLD	New Generic Top-Level Domain	Tên miền cấp cao dùng chung mới
PoP	Point of Presence	Vị trí vật lý nơi nhà cung cấp dịch vụ mạng hoặc mạng khác có thiết bị và cung cấp dịch vụ kết nối
PQC	Post-Quantum Cryptography	Các phương pháp mã hóa bảo mật trước các cuộc tấn công từ máy tính lượng tử
RFC	Request for Comments	Tài liệu đặc tả các giao thức, tiêu chuẩn và công nghệ sử dụng trên Internet
RNDC	Remote Name Daemon Control	Công cụ điều khiển BIND từ xa
RPZ	Response Policy Zone	Chính sách phản hồi zone
RTT	Round Trip Time	Thời gian gói dữ liệu đi và về
SRS-EPP	SRS Extensible Provisioning Protocol	Giao thức được sử dụng bởi các cơ quan đăng ký và nhà đăng ký để quản lý đăng ký tên miền
TCP	Transmission Control Protocol	Giao thức kết nối, đảm bảo việc truyền tải dữ liệu một cách đáng tin cậy trên Internet
TCP/IP	Transmission Control Protocol/Internet	Bộ giao thức truyền thông cơ bản cho mạng máy tính và Internet
TLD	Top-Level Domain	Tên miền cấp cao
TTL	Time to Live	Thời gian tồn tại của bản ghi DNS trong bộ nhớ đệm (Cache)
UDP	User Datagram Protocol	Giao thức không kết nối, truyền tải dữ liệu mà không cần xác nhận, thường được sử dụng trong truyền phát trực tuyến
VNIX	Viet Nam National Internet eXchange	Trạm trung chuyển Internet quốc gia Việt Nam
VNNIC	Viet Nam Internet Network Information	Trung tâm Internet Việt Nam
ZSK	Zone Signing Key	Khóa ký zone sử dụng trong DNSSEC

DANH MỤC HÌNH VẼ

Hình 1: Hệ thống tên miền (DNS) 14
Hình 2: Vai trò quan trọng của DNS trong Internet 15
Hình 3: Cấu trúc không gian tên miền 18
Hình 4: Zone tên miền 18
Hình 5: Chuyển giao tên miền (Delegation) 19
Hình 6: Quy trình đăng ký tên miền quốc gia .VN 24
Hình 7: Tên miền và DNS 25
Hình 8: Mô hình mạng hiện đại, kết nối đa hướng BGP Multihome 27
Hình 9: Cấu trúc gói tin DNS 29
Hình 10: Định dạng header của gói tin DNS 29
Hình 11: Định dạng phần câu hỏi 32
Hình 12: Định dạng phần phản hồi 33
Hình 13: Giao thức DNS trong mô hình TCP/IP 33
Hình 14: Các bước truy vấn tên miền www.vnnic.vn 35
Hình 15: Truy vấn đệ quy 36
Hình 16: Truy vấn lặp/không đệ quy 38
Hình 17: Chuyển giao tên miền ngược 38
Hình 18: Mô hình Master-Slave 42
Hình 19: Khai báo tên miền ngược IPv6 51
Hình 20: Truy vấn trên hệ thống DNS IPv4, IPv6 52
Hình 21: Cơ chế mở rộng DNS cho IPv6 52
Hình 22: Các phương thức triển khai DNS với IPv6 53
Hình 23: Bản đồ kiểm tra DNS bằng công cụ DNSChecker 63
Hình 24: Kiểm tra DNSSEC bằng công cụ DNSviz 63
Hình 25: Kiểm tra DNS bằng công cụ DNS Watch by VNNIC 64
Hình 26: Kiểm tra DNS bằng công cụ Zonemaster 64
Hình 27: Công cụ flush cache DNS của Google 78
Hình 28: Công cụ flush cache của Cloudflare 78
Hình 29: Kỹ thuật định tuyến Anycast 82
Hình 30: So sánh Anycast, Unicast, Multicast và Broadcast 82
Hình 31: Bản đồ các máy chủ DNS Root toàn cầu 83
Hình 32: Mô hình local cluster trong Anycast 84
Hình 33: Mô hình global cluster trong Anycast 85
Hình 34: Tấn công DNS Cache Poisoning 87
Hình 35: Quá trình tấn công DNS Cache Poisoning 88
Hình 36: Tấn công từ chối dịch vụ DoS/DDoS 89
Hình 37: Tấn công khuếch đại DNS Amplification 90
Hình 38: Tấn công DNS Hijacking 91
Hình 39: Tấn công DNS Tunneling 92
Hình 40: Tấn công Phantom Domain Attack 92
Hình 41: Tấn công Random Subdomain Attack 93
Hình 42: Tấn công Domain Hijacking 93
Hình 43: Ứng dụng ML phân tích truy vấn DNS phát hiện mã độc 95
Hình 44: Mô hình triển khai DNS Firewall in-band 96
Hình 45: Mô hình triển khai DNS Firewall out-band 96
Hình 46: Hệ thống DNS không sử dụng RPZ 97
Hình 47: Hệ thống DNS sử dụng RPZ 97
Hình 48: Hiệu năng phần mềm BIND9 khi tắt & bật logging 99
Hình 49: Định dạng dòng nhật ký truy vấn DNS phần mềm BINDH9 99
Hình 50: Mô hình chức năng của các thành phần trong công cụ ELK 100

Hình 51: Đồ thị giám sát tổng quan hoạt động DNS sử dụng ELK 101
Hình 52: Đồ thị giám sát chi tiết hoạt động DNS sử dụng ELK 102
Hình 53: Đồ thị giám sát hoạt động DNS sử dụng DSC 102
Hình 54: Đồ thị giám sát hoạt động DNS sử dụng DSC (kết hợp Grafan) 103
Hình 55: Mô hình logic triển khai C-DNS 104
Hình 56: Đồ thị giám sát tổng quan hoạt động DNS sử dụng C-DNS 104
Hình 57: Mã hoá DNS 106
Hình 58: DNS over TLS (DoT) 107
Hình 59: DNS over HTTPS (DoH) 108
Hình 60: Oblivious DOH (ODoH) 109
Hình 61: Các vấn đề bảo mật trong hoạt động của hệ thống DNS 113
Hình 62: Phân biệt DNS Security và DNSSEC 114
Hình 63: Quá trình truy vấn và được xác thực với DNSSEC 115
Hình 64: Tỉ lệ xác thực DNSSEC theo quốc gia (APNIC) 119
Hình 65: Các thành phần trong triển khai DNSSEC 119
Hình 66: Mô hình có CDN và không có CDN 128
Hình 67: Mô hình kiến trúc CDN 128
Hình 68: DNS và CDN 130
Hình 69: Minh hoạ hoạt động của GeoDNS 131
Hình 70: Quá trình phân giải trước khi CNAME Flattening 132
Hình 71: Quá trình phân giải sau khi CNAME Flattening 133
Hình 72: Multi-CDN 134
Hình 73: Mô hình máy chủ quản lý tên miền 136
Hình 74: Mô hình máy chủ tên miền đệm 137
Hình 75: Mô hình Lab-1 – Authortitative DNS Server 138
Hình 76: Ví dụ minh họa cập nhật bản ghi NS 152
Hình 77: Ví dụ minh họa tra cứu WHOIS 152
Hình 78: Ví dụ minh họa kết quả tra cứu WHOIS 153
Hình 79: Kiểm tra tên miền bằng công cụ DNS Watch by VNNIC 153
Hình 80: Mô hình Lab-2 - DNS Caching 154
Hình 81: Định dạng log phần mềm BIND 158
Hình 82: Thiết lập máy chủ phân giải DNS trên HĐH Windows (1) 159
Hình 83: Thiết lập máy chủ phân giải DNS trên HĐH Windows (2) 159
Hình 84: Thiết lập máy chủ phân giải DNS trên HĐH Windows (3) 160
Hình 85: Thiết lập máy chủ phân giải DNS trên HĐH Unix/Linux 160
Hình 86: Mô hình Lab-3 - Truy vấn xác thực DNSSEC 161
Hình 87: Các mốc thời gian trong quá trình thay khóa DNSSEC 166
Hình 88: Timeline quá trình thay khóa DNSSEC với pre-public 167
Hình 89: Timeline quá trình thay khóa DNSSEC với double-signature 168
Hình 90: Định dạng bản ghi ký chuyển giao DS – Delegation Signer 168
Hình 91: Hình minh họa tra cứu WHOIS 170
Hình 92: Kết quả kiểm tra DNSSEC bằng công cụ DNSviz 171

LỜI NÓI ĐẦU

Hệ thống tên miền (Domain Name System – DNS) là một trong những nền tảng hạ tầng thiết yếu của Internet, đảm nhiệm chức năng phân giải tên miền thành địa chỉ IP, giúp người dùng truy cập các dịch vụ trực tuyến một cách thuận tiện, nhanh chóng và hiệu quả. Trong bối cảnh Internet không ngừng phát triển về quy mô và tính phức tạp, DNS ngày càng đóng vai trò then chốt trong việc duy trì hoạt động ổn định, an toàn và thông suốt của toàn bộ hệ thống mạng toàn cầu.

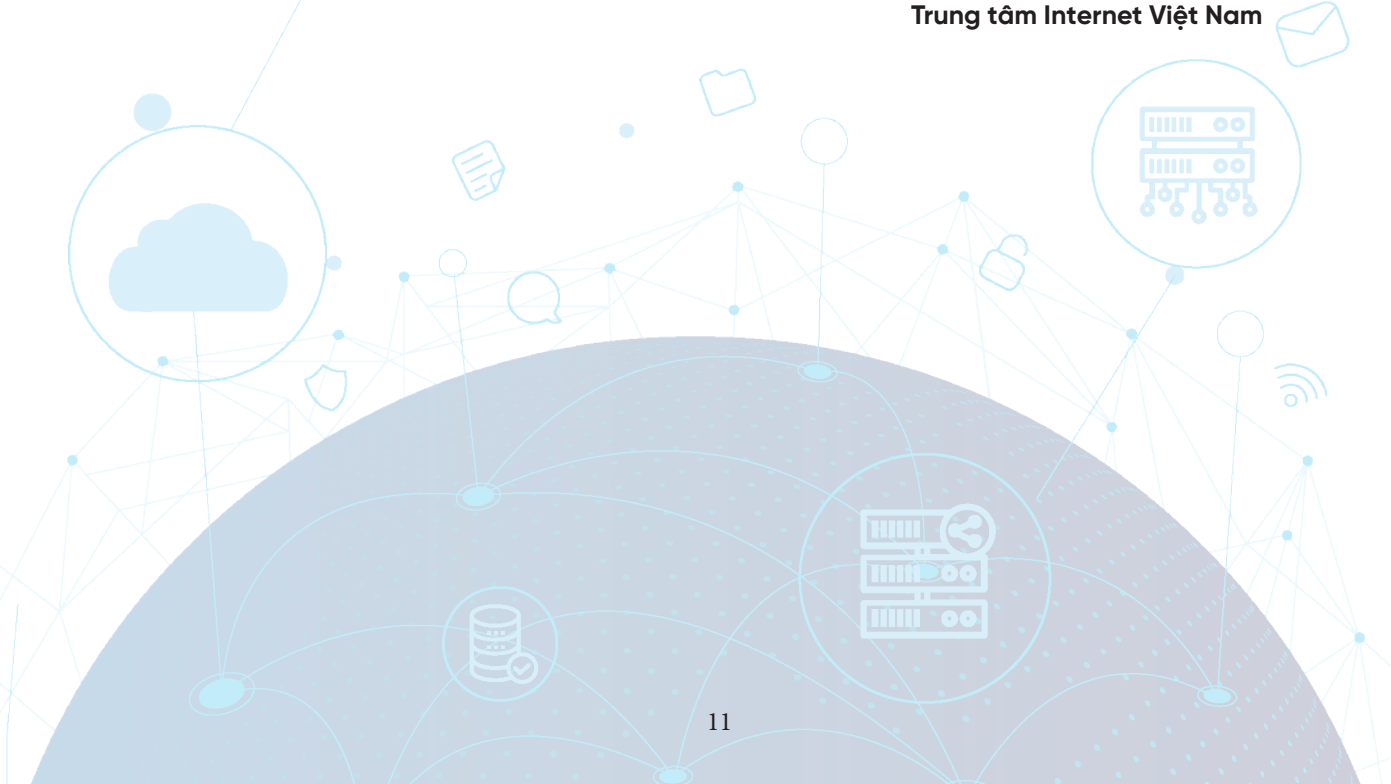
Trên thế giới, đã có nhiều tài liệu chuyên sâu dưới dạng sách cung cấp kiến thức toàn diện về DNS, từ lý thuyết nền tảng đến hướng dẫn triển khai và bảo mật thực tế. Các cuốn sách kinh điển như DNS and BIND (Cricket Liu & Paul Albitz), DNS Security (Allan Liska & Geoffrey Stowe) hay Pro DNS and BIND 10 (Ron Aitchison) đều được giới chuyên môn đánh giá cao về tính hệ thống, cập nhật và khả năng ứng dụng thực tiễn trong quản trị hạ tầng mạng.

Tại Việt Nam, tuy đã có một số bài viết, tài liệu đào tạo và khóa học đề cập đến DNS, song các nội dung hiện nay chủ yếu mang tính phổ biến kiến thức, chưa hình thành được một hệ thống tài liệu chuyên sâu, bài bản và gắn với điều kiện triển khai thực tế trong nước. Điều này gây ra không ít khó khăn cho các cán bộ kỹ thuật, nhà quản trị hệ thống và chuyên gia an toàn thông tin trong việc tiếp cận, nâng cao năng lực, cũng như triển khai hiệu quả các mô hình DNS hiện đại.

Trước yêu cầu đảm bảo an toàn, ổn định và bền vững cho hạ tầng Internet quốc gia, việc xây dựng một tài liệu kỹ thuật chuyên môn về DNS có tính hệ thống, toàn diện, cập nhật và phù hợp với đặc thù kỹ thuật – quản lý tại Việt Nam là hết sức cần thiết. Cuốn sách này được biên soạn với mục tiêu cung cấp tri thức chuyên sâu về kiến trúc, quản trị, vận hành, tối ưu và bảo mật hệ thống DNS, đồng thời cập nhật các xu hướng công nghệ mới như DNS trong môi trường IPv6, DNSSEC, Anycast, CDN, DNS-over-HTTPS/TLS; cũng như ứng dụng, tích hợp DNS với các công nghệ mới như 5G, IoT, AI, Blockchain, Edge-Computing, ... Bên cạnh các nội dung lý thuyết, sách còn tập trung vào các hướng dẫn triển khai thực tiễn, gắn với nhu cầu và điều kiện kỹ thuật tại các cơ quan, tổ chức và doanh nghiệp tại Việt Nam.

Chúng tôi kỳ vọng cuốn sách sẽ là tài liệu tham khảo hữu ích, góp phần nâng cao năng lực chuyên môn cho đội ngũ cán bộ kỹ thuật, chuyên gia bảo mật và nhà hoạch định kiến trúc, công nghệ trong việc thiết kế, triển khai và vận hành hệ thống DNS, từ đó tăng cường độ tin cậy, khả năng phục hồi và bảo vệ hạ tầng Internet quốc gia trước các thách thức mới của kỷ nguyên số.

Trung tâm Internet Việt Nam



PHẦN 1

QUẢN TRỊ VẬN HÀNH, TỐI ƯU HỆ THỐNG DNS

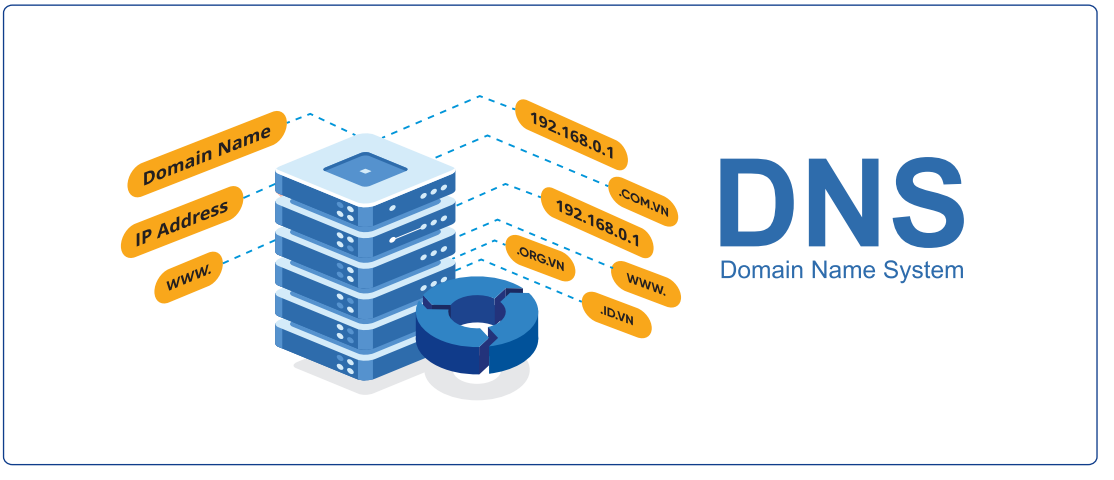
I

GIỚI THIỆU VỀ DNS

1. Khái niệm DNS

Hệ thống tên miền (DNS - Domain Name System) là một trong những thành phần cốt lõi, không thể thiếu của hạ tầng mạng Internet hiện đại. DNS được thiết kế nhằm giải quyết một vấn đề tưởng chừng đơn giản nhưng mang tính nền tảng, đó là ánh xạ giữa và tên miền (một dạng định danh dễ hiểu và dễ ghi nhớ đối với con người) và địa chỉ IP (vốn là định danh duy nhất của các thiết bị trên mạng). Với vai trò như là "sổ danh bạ của Internet", DNS cho phép các thiết bị giao tiếp với nhau một cách hiệu quả thông qua tên miền thay vì địa chỉ IP phức tạp và khó nhớ.

Về mặt khái niệm, DNS là một hệ thống phân tán, được tổ chức theo mô hình cây phân cấp (hierarchical tree). Mỗi nút trên cây DNS đại diện cho một miền (domain) hoặc một tập hợp con các miền (subdomain), được quản lý bởi các máy chủ DNS (DNS Server hay còn gọi với tên khác là Name Server). Hệ thống này hoạt động dựa trên nguyên tắc phân quyền và chuyển giao phân tán, nơi mỗi cấp của cây DNS chịu trách nhiệm lưu trữ và cung cấp thông tin ánh xạ cho một miền cụ thể. Điều này không chỉ giúp DNS có khả năng mở rộng quy mô để phục vụ hàng tỷ người dùng, thiết bị trên toàn cầu mà còn đảm bảo tính ổn định và khả năng phục hồi trước các sự cố mạng.

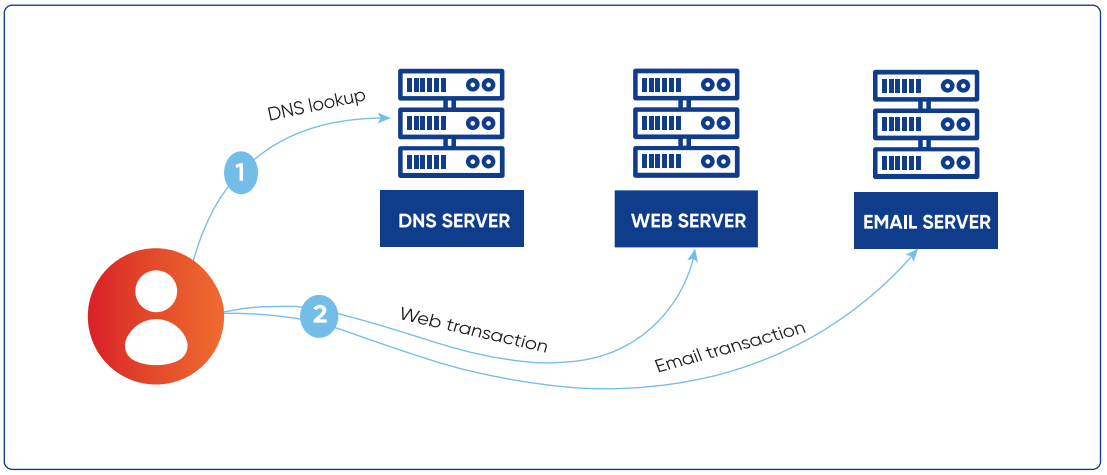


Hình 1: Hệ thống tên miền (DNS)

Chức năng chính của hệ thống máy chủ DNS là cung cấp dịch vụ phân giải tên miền (name resolution). Khi một người dùng nhập tên miền vào trình duyệt Internet, chẳng hạn như tên miền www.vnnic.vn, máy chủ DNS sẽ chuyển đổi tên miền này thành địa chỉ IP của máy chủ quản lý website www.vnnic.vn tương ứng, giúp thiết bị truy cập đến dịch vụ mong muốn. Quá trình này diễn ra thông qua một chuỗi các truy vấn (query), được xử lý thông qua các máy chủ DNS ở các cấp khác nhau.

2. Vai trò và tầm quan trọng của DNS trong Internet

Hệ thống DNS được coi là thành phần cốt lõi, "trái tim" của Internet. DNS không chỉ đóng vai trò trung tâm trong việc duy trì hoạt động của mạng Internet toàn cầu mà còn là thành phần không thể thiếu trong mọi dịch vụ trực tuyến trên không gian mạng.



Hình 2: Vai trò quan trọng của DNS trong Internet

DNS có nhiệm vụ phân giải tên miền thành địa chỉ IP và ngược lại, chức năng của DNS về căn bản là một hệ thống giúp cho việc chuyển đổi các tên miền mà con người dễ ghi nhớ (dạng ký tự, ví dụ www.vnnic.vn) sang địa chỉ IP vật lý (dạng số, ví dụ 123.11.5.19) tương ứng của tên miền đó. DNS giúp liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị trên Internet.

Khi mở một trình duyệt Web và nhập tên website, trình duyệt sẽ truy cập trực tiếp vào trang web mà không cần phải thông qua việc nhập địa chỉ IP của trang web. Quá trình "dịch" hay "phân giải" tên miền thành địa chỉ IP để cho trình duyệt hiểu và truy cập được vào website là công việc của một máy chủ DNS. Các máy chủ DNS tương tác qua lại với nhau để phân giải tên miền thành địa chỉ IP và ngược lại. Người sử dụng chỉ cần nhớ tên miền, không cần phải nhớ địa chỉ IP (địa chỉ IP là những con số rất khó nhớ).

Hầu hết mọi hoạt động trên Internet đều thông qua hệ thống DNS, do đó hệ thống DNS có vai trò rất quan trọng trong Internet. Ngoài chức năng cốt lõi, hệ thống DNS còn đóng vai trò trung tâm trong bảo mật mạng và các công nghệ mới.

Các nội dung chi tiết sẽ được trình bày ở các phần tiếp theo trong cuốn sách này.

3. Lịch sử phát triển của DNS

Vào những năm 1970, mạng máy tính ARPANET, tiền thân của Internet ngày nay, chỉ bao gồm vài trăm máy tính được kết nối với nhau. Khi đó, việc ánh xạ giữa tên máy và địa chỉ IP được thực hiện thông qua một tệp tin duy nhất mang tên HOSTS.TXT. Tệp tin này lưu trữ thông tin ánh xạ giữa tên máy và địa chỉ IP của tất cả các máy tính trên mạng ARPANET. Việc quản lý và cập nhật tệp HOSTS.TXT được giao cho SRI-NIC (Stanford Research Institute's Network Information Center), tổ chức chịu trách nhiệm lưu trữ và phân phối tệp tin này tới các máy tính khác trên mạng.

Quá trình cập nhật tệp HOSTS.TXT diễn ra thủ công: các quản trị viên mạng thường gửi email thông báo thay đổi tới SRI-NIC và tải về phiên bản mới thông qua giao thức FTP. Công việc này được thực hiện từ một đến hai lần mỗi tuần. Tuy nhiên, khi mạng ARPANET phát triển, với sự gia tăng nhanh chóng số lượng máy tính được kết nối, cơ chế sử dụng tệp HOSTS.TXT dần trở nên không phù hợp. Kích thước tệp tin tăng lên tỷ lệ thuận với số lượng máy tính trên mạng, dẫn đến nhiều vấn đề nghiêm trọng như:

- Quá tải về lưu lượng và tải xử lý: Máy chủ của SRI-NIC không thể chịu được tải lớn khi các máy tính liên tục gửi yêu cầu cập nhật tệp HOSTS.TXT.
- Xung đột về tên máy: Không có cơ chế ngăn chặn người dùng đặt trùng tên máy trên mạng. Điều này dẫn đến tình trạng các dịch vụ quan trọng có thể bị gián đoạn khi xảy ra xung đột tên.
- Khó khăn trong việc bảo trì: Việc cập nhật tệp HOSTS.TXT trở nên phức tạp khi mạng mở rộng. Trước khi tệp tin mới được phân phối, địa chỉ IP hoặc tên máy có thể đã thay đổi, làm tăng nguy cơ thông tin không đồng bộ kịp thời.

Những hạn chế này cho thấy cơ chế sử dụng tệp HOSTS.TXT không còn đáp ứng được yêu cầu của một mạng máy tính đang phát triển nhanh chóng.

- Quản lý phi tập trung: Phân phối dữ liệu trên nhiều máy chủ để tránh tình trạng quá tải.
- Cập nhật cục bộ: Cho phép mỗi máy chủ tự quản lý dữ liệu của mình một cách hiệu quả.
- Phân cấp không gian tên miền: Sử dụng cấu trúc phân tầng để đảm bảo tính duy nhất của tên miền.

Hệ thống mới này chính là DNS (Domain Name System), được phát triển bởi Paul Mockapetris thuộc Viện Nghiên cứu Kỹ thuật Thông tin. Năm 1984, Paul Mockapetris công bố hai tài liệu tiêu chuẩn là RFC 882 và RFC 883, mô tả chi tiết nguyên lý hoạt động của hệ thống DNS.

Hệ thống DNS trên toàn cầu nói chung, được quản lý và hoạt động dưới các chính sách và tiêu chuẩn được quy định bởi ICANN, tổ chức chịu trách nhiệm thiết lập các quy định về việc sử dụng tên miền và các nguồn tài nguyên Internet. IANA, dưới sự quản lý của ICANN, thực hiện các nhiệm vụ kỹ thuật cần thiết như phân bổ địa chỉ IP và quản lý thông tin cấu hình cho các máy chủ DNS Root, đảm bảo hệ thống DNS hoạt động hiệu quả và bảo mật.

ICANN (Internet Corporation for Assigned Names and Numbers) là một tổ chức phi lợi nhuận, độc lập, có trụ sở tại California, Hoa Kỳ, được thành lập vào năm 1998 với nhiệm vụ quản lý và điều phối các tên miền và số hiệu mạng trong hệ thống Internet toàn cầu. ICANN chịu trách nhiệm quản lý tất cả các tên miền cấp cao (TLDs - Top-Level Domains), bao gồm các generic-TLD (gTLDs) như .com, .org; các TLD mã quốc gia (ccTLDs) như .vn, .us, .uk; các tên miền sponsored-TLD (sTLDs) như .aero, .museum và các tên miền dùng chung mới hay còn gọi là new gTLD như .tech, .store, .blog, .online, ... ICANN đóng vai trò thiết lập các quy tắc và chính sách liên quan đến quản lý tên miền, giải quyết các tranh chấp tên miền, và giám sát các quy trình đăng ký tên miền qua hợp đồng với các nhà đăng ký hợp pháp (http://www.icann.org/en/registrars/accredited-list.html). ICANN cũng duy trì danh sách các máy chủ DNS Root và giám sát hoạt động của chúng để đảm bảo tính ổn định và bảo mật của hệ thống DNS toàn cầu. Ngoài ra, ICANN còn có trách nhiệm quyết định việc cấp phép và ủy quyền cho các TLD mới, giúp mở rộng hệ thống DNS và đáp ứng nhu cầu phát triển của Internet.

IANA (Internet Assigned Numbers Authority) là tên gọi của một tập hợp các chức năng kỹ thuật thiết yếu trong việc quản lý, phân phối các tài nguyên quan trọng của Internet, bao gồm địa chỉ IP, số hiệu mạng (ASN), thông số giao thức và quản lý tên miền cấp cao (TLD). Các chức năng này hiện được thực hiện bởi Public Technical Identifiers (PTI) - một công ty con của ICANN, được thành lập để đảm bảo tính minh bạch và trách nhiệm giải trình trong việc vận hành các chức năng IANA.

IANA đóng vai trò then chốt trong việc duy trì sự ổn định và an toàn của hạ tầng Internet toàn cầu. Cụ thể, IANA chịu trách nhiệm duy trì và cập nhật danh sách tất cả các tên miền cấp cao (TLD), bao gồm cả các tên miền mã quốc gia (ccTLD), đảm bảo quá trình phân bổ và quản lý được thực hiện công bằng và chính xác. Bên cạnh đó, IANA còn quản lý các bản ghi liên quan đến hệ thống máy chủ DNS gốc (DNS Root) và zone tên miền gốc (root zone), giúp đảm bảo thông tin về các TLD và máy chủ DNS luôn được cập nhật đầy đủ, kịp thời và chính xác.

Cả ICANN và IANA (thông qua PTI) đều đóng vai trò quan trọng trong việc bảo vệ tính toàn vẹn, độ tin cậy và khả năng mở rộng của hệ thống DNS toàn cầu. Nhờ đó, các tài nguyên Internet được quản lý hiệu quả, góp phần hỗ trợ sự phát triển bền vững và ổn định của Internet trên toàn thế giới.

II

CÁC KHÁI NIỆM CƠ BẢN

1. Tên miền và địa chỉ IP

1.1. Tên miền

Như đã giới thiệu ở trên, hệ thống DNS là một hệ thống phân tán, được tổ chức theo mô hình cây phân cấp (hierarchical tree). Mỗi một nút trong cấu trúc hình cây của DNS được gắn với một nhãn (label) nhất định. Nhãn này có thể chứa tối đa 63 ký tự, bao gồm các ký tự A-Z, a-z, 0-9 và dấu gạch ngang "-". Gốc của cây không có nhãn và được biểu diễn bằng dấu ".". Khi các nhãn trên một nhánh của cây được viết theo thứ tự từ xa nhất đến gốc và phân cách nhau bằng dấu ".", ta sẽ biểu diễn được một tên miền. Ví dụ, trong không gian tên miền có các nhãn như www, vnnic, vn. Từ các nhãn này, ta có thể tạo ra các tên miền như "www.vnnic.vn." hoặc "vnnic.vn.".

Một tên miền đầy đủ (Fully Qualified Domain Name - FQDN) hay còn gọi là tên miền tuyệt đối (Absolute Domain Name), là một chuỗi các nhãn từ nút đó đến gốc, được phân cách bởi dấu "." và kết thúc bằng dấu ".". Ví dụ, tên miền "www.vnnic.vn." là một tên miền đầy đủ, trong khi "www.vnnic.vn" không phải là tên miền đầy đủ vì thiếu dấu "." ở cuối cùng. Các tên miền không được kết thúc bằng dấu "." được gọi là tên miền tương đối (Relative Domain Name). Trong các trình duyệt web và hệ điều hành hiện nay đều tự động thêm hoặc bỏ qua dấu "." ở cuối tên miền, nên người dùng không thấy sự khác biệt khi gõ tên miền đầy đủ và tên miền tương đối. Tuy nhiên về mặt kỹ thuật, đặc biệt khi phát triển phần mềm, cấu hình máy chủ cần viết tên miền ở dạng tuyệt đối (có dấu "." ở cuối) để tránh trường hợp các hệ thống có thể gán thêm một domain suffix (hậu tố), làm sai lệch kết quả hoạt động.

Mỗi tên miền có thể chứa thông tin về một máy chủ (host) hoặc về cấu trúc cấp dưới (subdomain) của nó. Việc tìm kiếm thông tin liên quan đến tên miền phụ thuộc vào ứng dụng sử dụng nó. Ví dụ, ứng dụng WEB, MAIL hoặc FTP sử dụng tên miền sẽ trả về địa chỉ IP của máy chủ để kết nối đến.

1.2. Địa chỉ IP

Địa chỉ IP (Internet Protocol Address) là một chuỗi số hoặc ký tự dùng để định danh duy nhất mỗi thiết bị trong mạng Internet hoặc mạng nội bộ. Nó giống như "địa chỉ nhà" của thiết bị trên không gian mạng, giúp các thiết bị có thể giao tiếp và truyền dữ liệu qua lại. Có hai loại địa chỉ IP phổ biến hiện nay là IPv4 và IPv6.

- **IPv4 (Internet Protocol version 4)** là phiên bản được sử dụng rộng rãi từ khi Internet ra đời, sử dụng địa chỉ 32-bit và hiển thị dưới dạng bốn nhóm số thập phân ngăn cách nhau bởi dấu chấm ".", ví dụ: 192.168.1.1. Tuy nhiên, do sự bùng nổ của các thiết bị kết nối, IPv4 đã cạn kiệt vào năm 2011, hai khu vực còn IPv4 là APNIC, AFNIC chỉ cấp phát hạn chế trong giai đoạn quá độ, dự kiến cạn kiệt hoàn toàn vào năm 2027-2028.
- **IPv6 (Internet Protocol version 6)** ra đời để giải quyết vấn đề này, sử dụng địa chỉ 128-bit với không gian địa chỉ lớn hơn rất nhiều. IPv6 được biểu diễn bằng tám nhóm số thập lục phân, ví dụ: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

DNS đóng vai trò như một "người phiên dịch", chuyển đổi các tên miền dễ nhớ (như www.vnnic.vn) thành địa chỉ IP mà các thiết bị sử dụng để giao tiếp. Khi người dùng nhập một tên miền vào trình duyệt, hệ thống DNS sẽ thực hiện phân giải tên miền để tìm ra địa chỉ IP tương ứng, từ đó kết nối tới máy chủ cung cấp dịch vụ.

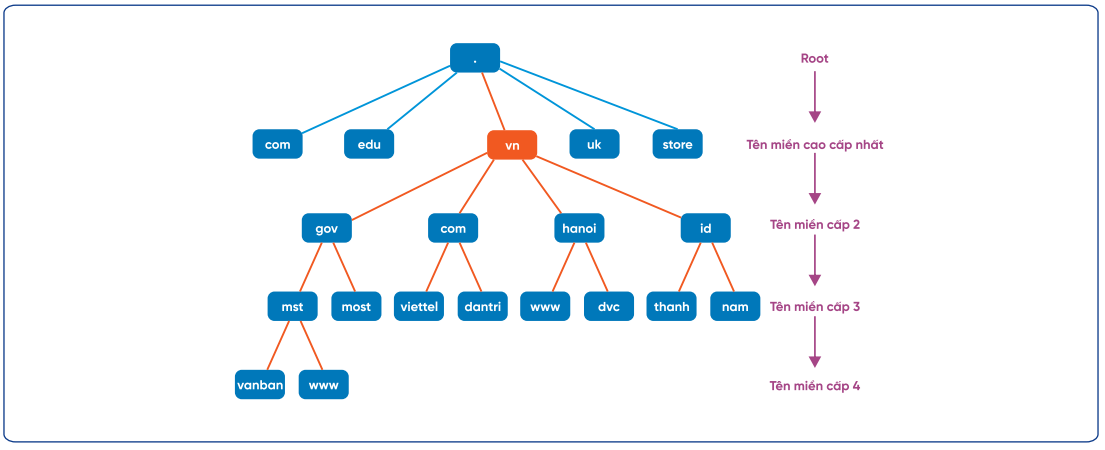
2. Cấu trúc phân cấp tên miền

2.1. Không gian tên miền

Hệ thống tên miền là một cơ sở dữ liệu phân tán, cơ sở dữ liệu này có các đặc điểm:

- Cho phép quản lý một cách cục bộ các phần khác nhau trong toàn bộ hệ thống tên miền.
- Dữ liệu trong mỗi phần này có thể được truy cập trên toàn mạng thông qua cơ chế client-server.
- Cơ sở dữ liệu này đảm bảo tính ổn định và đồng nhất của hệ thống tên miền.

Trong hệ thống tên miền, không gian tên miền (domain name space) là một cấu trúc phân cấp hình cây, được sử dụng để tổ chức và quản lý các tên miền.



Hình 3: Cấu trúc không gian tên miền

Theo cấu trúc hình cây ở trên, tên miền được phân thành các cấp độ:

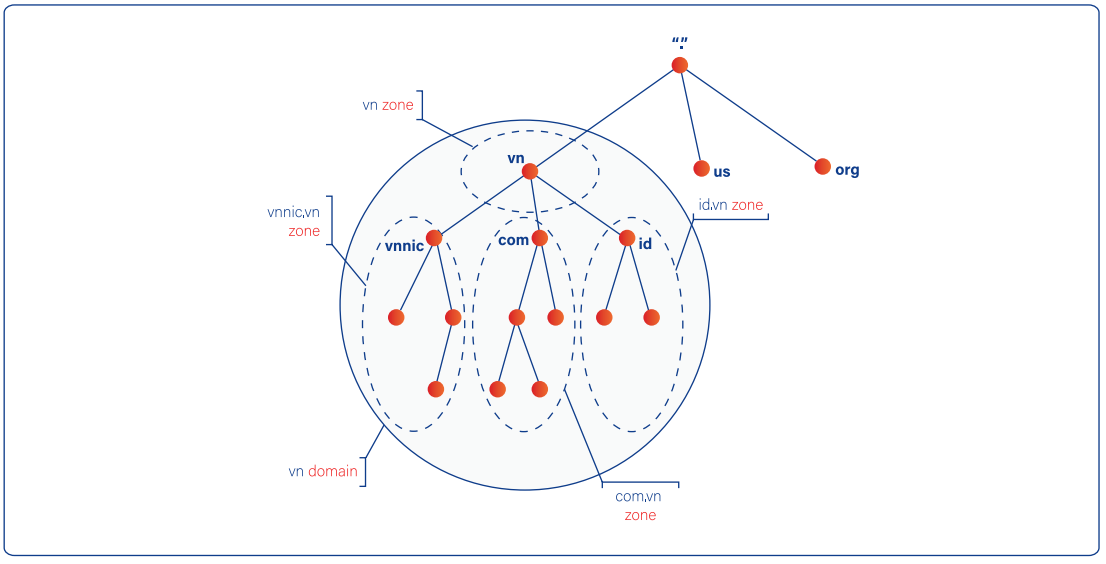
- Tên miền gốc (Root Domain): Là cấp cao nhất trong hệ thống tên miền, được biểu thị bằng dấu ".". Tên miền gốc không có tên cụ thể, nhưng là điểm khởi đầu cho tất cả các tên miền.
- Tên miền cấp cao nhất (Top-Level Domain - TLD): Là tên miền ngay dưới gốc (root), ví dụ: .vn. .us, .com, .net, ...
- Tên miền cấp hai (Second-Level Domain): Là tên miền nằm dưới TLD, ví dụ: vnnic.vn, vnpt.vn, viettel.vn, ...
- Tên miền cấp ba (Third-Level Domain): Là tên miền dưới cấp hai, ví dụ: mail.vnnic.vn.
- Tên miền cấp bốn (Fourth-Level Domain): Là tên miền dưới cấp ba, ví dụ: mx.mail.vnnic.vn.
- Các cấp dưới khác: Có thể có nhiều cấp dưới khác nữa, tùy theo nhu cầu tổ chức và quản lý.

Mô hình phân cấp này đảm bảo sự duy nhất của mỗi tên miền và hỗ trợ việc quản lý cũng như tra cứu thông tin một cách hiệu quả.

2.2. Máy chủ tên miền và zone tên miền

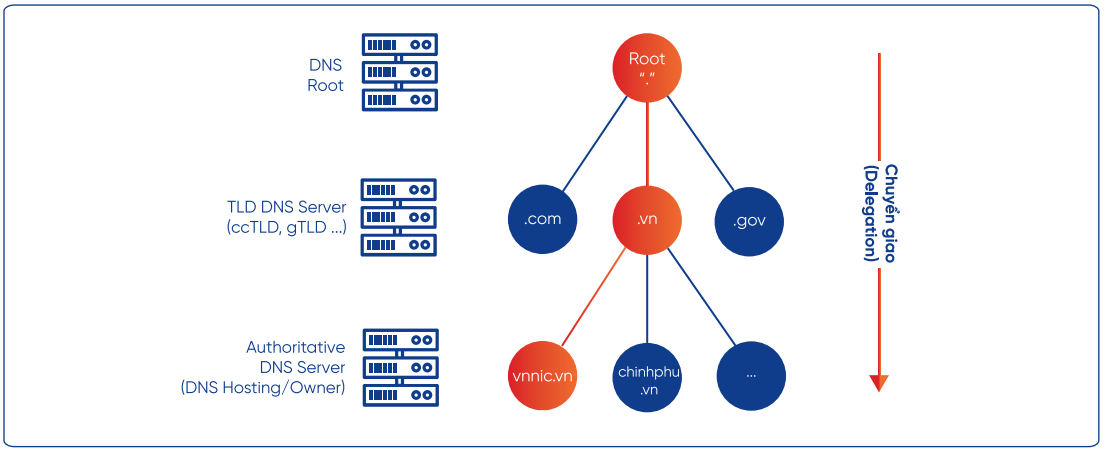
Máy chủ tên miền (DNS Server hay Name Server) là hệ thống lưu trữ thông tin về không gian tên miền và thực hiện phân giải tên miền thành địa chỉ IP. Máy chủ tên miền sẽ chứa toàn bộ thông tin về một phần trong không gian tên miền và phần thông tin về tên miền do máy chủ tên miền quản lý được gọi là zone. Khi máy chủ tên miền quản lý các thông tin về tên miền trong một zone thì máy chủ này được coi là có thẩm quyền (authority) với zone đó. Một máy chủ tên miền có thể chứa thông tin của nhiều phần trong không gian tên miền, điều này có nghĩa là nó có thể có quyền với nhiều zone.

Zone là một phần của hệ thống DNS, nơi lưu trữ thông tin về tên miền và các bản ghi tương ứng, như địa chỉ IP, máy chủ email và các loại bản ghi khác liên quan đến tên miền đó.



Hình 4: Zone tên miền

Tuy nhiên zone không lưu trữ các thông tin của các tên miền con (subdomain) đã được chuyển giao. Ví dụ, tên miền .vn có thể có các tên miền con cấp thấp hơn như fpt.vn, vnn.vn, ... được chuyển giao cho các tổ chức đăng ký sử dụng tên miền đó. Tên miền .vn sẽ lưu giữ thông tin của tất cả các tên miền con của nó. Tuy nhiên, zone .vn sẽ không lưu giữ các thông tin của các tên miền con như fpt.vn, vnn.vn vì các tên miền này đã được chuyển giao cho các tổ chức quản lý. Dữ liệu chứa trong zone .vn chỉ chứa các thông tin về tên miền dưới .vn nhưng không được chuyển giao.



Hình 5: Chuyển giao tên miền (Delegation)

Tương ứng với mỗi cấp trong cấu trúc phân cấp của hệ thống tên miền sẽ được quản lý bởi các máy chủ DNS, gồm: máy chủ tên miền gốc (DNS Root), máy chủ tên miền cấp cao nhất (TLD DNS Server), máy chủ tên miền có thẩm quyền (Authoritative DNS Server).

3. Các thành phần của hệ thống tên miền

Hệ thống DNS được xây dựng từ nhiều thành phần hoạt động tương tác chặt chẽ với nhau, tạo nên một cơ chế phân giải tên miền hiệu quả. Mỗi thành phần đảm nhận những vai trò và chức năng riêng biệt trong quá trình phân giải tên miền, đảm bảo tính chính xác, tin cậy và khả năng mở rộng của toàn hệ thống. Các thành phần chính của hệ thống DNS gồm:

(1) Không gian tên miền (Domain Name Space): Đây là cấu trúc phân cấp của tên miền, được hình thành như một cây đảo ngược. Đỉnh của cây là tên miền gốc (Root domain), được biểu thị bằng dấu chấm (.). Bên dưới tên miền gốc là các tên miền cấp cao nhất (Top-Level Domains - TLDs) như .vn, .us, .com, .net, ... Dưới TLD là các tên miền cấp hai (Second-Level Domains - SLDs), thường là tên của tổ chức hoặc cá nhân (ví dụ: vnnic.vn, vnpt.vn, viettel.vn, ...). Các tên miền có thể có thêm các tên miền con (subdomains) để phân chia và quản lý các phần khác nhau.

(2) Máy chủ tên miền (DNS Server hoặc Name Server): Đây là các máy chủ lưu trữ thông tin DNS cho một hoặc nhiều miền và trả lời các truy vấn DNS để cung cấp địa chỉ IP tương ứng với một tên miền. Có nhiều loại máy chủ tên miền trong hệ thống DNS phân cấp:

- *Máy chủ gốc (DNS Root hoặc Root Name Server):* Là các máy chủ tên miền cấp độ cao nhất trong cấu trúc phân giải tên miền. Chúng không lưu trữ thông tin về các tên miền cụ thể mà chỉ cung cấp thông tin về các máy chủ tên miền cấp dưới. Có 13 máy chủ tên miền gốc chính, được phân phối trên toàn cầu để đảm bảo tính khả dụng và độ tin cậy. Các máy chủ này được đánh dấu bằng các ký tự từ A đến M.
- *Máy chủ tên miền cấp cao nhất (TLD DNS Server):* Là các máy chủ tên miền quản lý thông tin các tên miền cấp cao nhất (TLD) và các tên miền con bên dưới TLD mà chúng quản lý. Máy chủ TLD DNS Server gồm có các máy chủ gTLD DNS Server (quản lý thông tin tên miền cấp cao dùng chung) và các máy chủ ccTLD DNS Server (quản lý thông tin tên miền cấp cao mã quốc gia và các tên miền con). Ví dụ, máy chủ .vn sẽ có thông tin về tên miền .vn, .com.vn, .net.vn, ... và các tên miền con như .vnpt.vn, .viettel.vn, ...). Máy chủ TLD DNS Server cũng là một loại Authoritative DNS Server như trình bày dưới đây.
- *Máy chủ có thẩm quyền (Authoritative DNS Server):* Đây là thành phần có quyền kiểm soát cuối cùng và chịu trách nhiệm cung cấp thông tin chính xác cho các tên miền cụ thể. Là nơi lưu trữ dữ liệu chính thức của các miền (zone data), bao gồm các bản ghi tài nguyên (Resource Records - RR) như bản ghi A (ánh xạ tên miền sang địa chỉ IPv4), bản ghi MX (Mail Exchange) cho email và bản ghi NS (Name Server) để chỉ định các máy chủ DNS có thẩm quyền.
  Authoritative DNS Server không thực hiện truy vấn đệ quy mà chỉ cung cấp câu trả lời trực tiếp dựa trên dữ liệu được lưu trữ trong zone của nó. Vai trò của nó là đảm bảo tính toàn vẹn và chính xác của dữ liệu DNS. Hệ thống này được phân cấp, với mỗi tổ chức hoặc nhà cung cấp dịch vụ quản lý các miền mà họ sở hữu.

Một điểm quan trọng cần lưu ý là Authoritative DNS Server đóng vai trò trung tâm trong việc triển khai các công nghệ bảo mật DNS hiện đại, chẳng hạn như DNSSEC (Domain Name System Security Extensions). Bằng cách ký số các bản ghi DNS, DNSSEC giúp bảo vệ dữ liệu khỏi bị giả mạo, tăng cường tính an toàn cho các giao dịch trên mạng.

(3) Bộ phân giải DNS (DNS Resolver): Bộ phân giải DNS (DNS Resolver, hay còn gọi là Recursive Resolver), là thành phần đầu tiên mà người dùng tương tác khi thực hiện một truy vấn DNS. Đây là hệ thống trung gian, chịu trách nhiệm tiếp nhận yêu cầu phân giải tên miền từ người dùng (thông qua các ứng dụng như trình duyệt web) và truy vấn các máy chủ DNS khác để tìm ra địa chỉ IP hoặc thông tin liên quan đến tên miền. Khi người dùng nhập một tên miền vào trình duyệt, bộ phân giải DNS sẽ gửi yêu cầu đến các máy chủ DNS theo một quy trình nhất định để tìm ra địa chỉ IP tương ứng. Quá trình này thường bắt đầu bằng cách truy vấn máy chủ gốc, sau đó đến máy chủ TLD và cuối cùng là máy chủ có thẩm quyền cho miền đó. Để tăng tốc độ, các bộ phân giải DNS thường lưu trữ (cache) các kết quả truy vấn trước đó.

- **Lý do chỉ tồn tại 13 cụm máy chủ DNS Root:**

Vào thời kỳ đầu thiết kế DNS (những năm 1980), một giới hạn quan trọng là các phản hồi DNS sử dụng UDP chỉ được phép phản hồi gói tin có kích thước tối đa 512 byte dữ liệu (Quy định này được đề cập trong RFC 1035 – phiên bản phát hành năm 1987). Mục tiêu là để phản hồi DNS có thể truyền đi mà không bị phân mảnh bởi tầng IP.

Theo RFC 791 (giao thức IP), mọi thiết bị sử dụng IPv4 phải có khả năng tái lắp ghép gói tin IP (sau khi bị phân mảnh) lên đến 576 byte, bao gồm cả tiêu đề IP (IP header) và tiêu đề UDP. Khi trừ đi khoảng 60-64 byte tiêu đề, phần dữ liệu DNS thực tế chỉ còn ~512 byte.

Vào thời đó, nhiều thiết bị định tuyến (router) và tường lửa (firewall) không hỗ trợ tốt các gói UDP bị phân mảnh hay nói cách khác, các thiết bị này không thể tái lắp ghép các gói tin một cách hoàn chỉnh sau khi bị phân mảnh. Một gói DNS vượt quá 512 byte có thể bị chia thành nhiều mảnh IP, và nếu một mảnh bị mất, toàn bộ gói tin phản hồi truy vấn sẽ thất bại. Ngoài ra, nhiều thiết bị mạng hoặc các mạng của các tổ chức có thể chặn hoàn toàn các gói DNS bị phân mảnh. Vì vậy, các nhà thiết kế giao thức ưu tiên giữ phản hồi DNS trong giới hạn 512 byte.

Theo nguyên tắc hoạt động của DNS được thiết kế từ những ngày đầu tiên. Khi người dùng thực hiện một truy cập vào tên miền lần đầu tiên, trình phân giải DNS (resolver) sẽ khởi tạo một truy vấn và thực hiện truy vấn danh sách các máy chủ DNS Root nhằm xác thực (và cập nhật) với danh sách địa chỉ các máy chủ DNS Root mà trình phân giải có. Phản hồi từ truy vấn này – gọi là priming response, có dạng như sau:

```
;; QUESTION SECTION:
;.                      IN      NS
;; ANSWER SECTION:
.               518400  IN      NS      a.root-servers.net.
.               518400  IN      NS      b.root-servers.net.
.               518400  IN      NS      c.root-servers.net.
.               518400  IN      NS      d.root-servers.net.
.               518400  IN      NS      e.root-servers.net.
.               518400  IN      NS      f.root-servers.net.
.               518400  IN      NS      g.root-servers.net.
.               518400  IN      NS      h.root-servers.net.
.               518400  IN      NS      i.root-servers.net.
.               518400  IN      NS      j.root-servers.net.
.               518400  IN      NS      k.root-servers.net.
.               518400  IN      NS      l.root-servers.net.
.               518400  IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3600000   IN      A       198.41.0.4
b.root-servers.net.     3600000   IN      A       170.247.170.2
c.root-servers.net.     3600000   IN      A       192.33.4.12
d.root-servers.net.     3600000   IN      A       199.7.91.13
e.root-servers.net.     3600000   IN      A       192.203.230.10
f.root-servers.net.     3600000   IN      A       192.5.5.241
g.root-servers.net.     3600000   IN      A       192.112.36.4
h.root-servers.net.     3600000   IN      A       198.97.190.53
i.root-servers.net.     3600000   IN      A       192.36.148.17
j.root-servers.net.     3600000   IN      A       192.58.128.30
k.root-servers.net.     3600000   IN      A       193.0.14.129
l.root-servers.net.     3600000   IN      A       199.7.83.42
m.root-servers.net.     3600000   IN      A       202.12.27.33
```

(Danh sách máy chủ DNS Root trước đây, khi chưa triển khai IPv6 & chỉ có địa chỉ IPv4).

Trong đó, kích thước của từng phần trong gói tin phản hồi DNS chi tiết như sau:

- Danh sách bản ghi NS của các máy chủ DNS Root (A đến M)
- Địa chỉ IP (A record) tương ứng cho từng máy chủ
- Một phần tiêu đề DNS – DNS header: 12 byte
- Phần câu hỏi truy vấn - QUESTION SECTION: 5 byte

```
- root-label: 00, 1 byte;
- class, 2 bytes;
- qtype: 2 bytes.
```

Khi tính toán kích thước của từng bản ghi:

- Bản ghi NS đầu tiên thường chiếm khoảng 31 byte:

```
- root-label: 1 byte;
- ttl: 4 bytes;
- class: 2 bytes;
- type: 2 bytes;
- rdlength: 2 bytes
- nameserver name: <1>a<12>root-servers<3>net<0>: 20 bytes.
```

- Các bản ghi NS tiếp theo, nhờ kỹ thuật nén tên miền (DNS compression), chỉ chiếm khoảng 15 byte:

```
- root-label: 1 byte;
- ttl: 4 bytes;
- class: 2 bytes;
- type: 2 bytes;
- rdlength: 2 bytes
- nameserver name: <1><letter><compression pointer>: 4 bytes.
```

- Mỗi bản ghi A (địa chỉ IP) đi kèm chiếm khoảng 16 byte:

```
- nameserver name: <1><letter><compression pointer>: 2
bytes;
- ttl: 4 bytes;
- class: 2 bytes;
- type: 2 bytes;
- rdlength: 2 bytes;
- address: 4 bytes.
```

Từ các thông số chi tiết trên, chúng ta có thể có cái nhìn tổng quát như sau:

12	;; ->>HEADER<<-
5	;; QUESTION SECTION:
31 + 15n	;; ANSWER SECTION:
16m	;; ADDITIONAL SECTION:

Trong đó, n và m là số lượng máy chủ DNS Root (thông thường n = m), từ đó ta có thể tính giới hạn số máy chủ DNS Root cho phép là:

```
48 + 31n = 512
n =14.96
```

Từ phép tính trên có thể thấy rằng, số lượng máy chủ DNS Root có thể có tối đa 14 máy chủ, tuy nhiên nhằm đảm bảo an toàn và các rủi ro chưa lường trước trong vấn đề truyền các gói tin DNS trên Internet, lựa chọn 13 máy chủ DNS Root là một lựa chọn đảm bảo an toàn.

Do đó, con số 13 được chọn không phải ngẫu nhiên, mà là kết quả của một quá trình tối ưu kỹ lưỡng nhằm đảm bảo cho các hoạt động truy vấn, phản hồi truy vấn DNS một cách nhanh chóng, tin cậy và không bị gián đoạn. Trong thực tế, 13 máy chủ này được triển khai sử dụng công nghệ Anycast, cho phép tạo ra nhiều bản sao của các máy chủ DNS Root nhưng chỉ với 13 địa chỉ IP khác nhau và đặt khắp nơi trên thế giới. Do đó, thuật ngữ "13 cụm máy chủ DNS Root" thay cho "13 máy chủ DNS Root" sẽ phản ánh chính xác về hệ thống máy chủ DNS Root.

Ngày nay, với sự phát triển của các công nghệ mới như IPv6, DNSSEC, ... các phản hồi DNS có kích thước lớn hơn nhiều (phản hồi DNS liệt kê tất cả các máy chủ DNS Root – priming response gồm địa chỉ IPv4 và IPv6 có kích thước 811 byte, phản hồi DNSSEC có thể lên đến 1.097 byte, ...). Điều này có thể thực hiện được mà không bị giới hạn kích thước phản hồi DNS bằng cách áp dụng tiêu chuẩn mở rộng EDNS(0)[1] , cho phép mở rộng kích thước gói DNS lên tới 4096 byte (hoặc thậm chí lớn hơn trong một số trường hợp), giúp truyền tải các phản hồi DNS lớn, đặc biệt là khi sử dụng DNSSEC, IPv6 hoặc khi có các bản ghi DNS dài.

Mặc dù các tiêu chuẩn công nghệ hiện nay cho phép và hỗ trợ các phản hồi DNS với kích thước lớn hơn 512 byte, điều này đồng nghĩa với việc chúng ta có thể thêm số lượng "cụm" máy chủ DNS Root (không chỉ giới hạn ở con số 13), tuy nhiên điều này là không thực sự cần thiết, vì với sự hỗ trợ của công nghệ Anycast, có thể đặt hàng ngàn máy chủ DNS Root (instance) ở khắp nơi trên thế giới với cùng 1 địa chỉ IP mà không ảnh hưởng đến giới hạn 13 máy chủ DNS Root. Đồng thời, nếu thay đổi số lượng cụm máy chủ DNS Root, có thể ảnh hưởng đến mô hình, kiến trúc hoạt động và các thiết lập của các hệ thống khác trên Internet mà không mang lại hiệu quả vượt trội. Do đó hiện nay vẫn duy trì 13 cụm máy chủ DNS Root (13 tên máy chủ DNS Root).

[1] Extension Mechanisms for DNS, version 0 là một tiêu chuẩn mở rộng cho giao thức DNS, được giới thiệu trong RFC 2671. EDNS(0) cho phép mở rộng khả năng của DNS để hỗ trợ các tính năng mới và cải thiện hiệu suất so với giao thức DNS truyền thống.

III

QUẢN LÝ, ĐĂNG KÝ TÊN MIỀN, IP TẠI VIỆT NAM

1. Quản lý, đăng ký tên miền

1.1. Quản lý tên miền ".vn"

Tên miền ".vn" là tên miền quốc gia của Việt Nam, được quản lý bởi Trung tâm Internet Việt Nam (VNNIC), đơn vị trực thuộc Bộ Khoa học và Công nghệ. VNNIC chịu trách nhiệm cấp phát, duy trì, và giám sát tất cả các hoạt động liên quan đến tên miền ".vn", bao gồm việc quản lý, vận hành hệ thống máy chủ tên miền (DNS) quốc gia ".vn", đảm bảo tính hợp pháp và bảo mật cho các tên miền đăng ký dưới đuôi ".vn". VNNIC cũng chịu trách nhiệm phối hợp với các Nhà đăng ký tên miền (registrars) để thực hiện đăng ký tên miền cho các cá nhân và tổ chức.

1.2. Đăng ký tên miền ".vn"

1.2.1. Quy định về đăng ký, sử dụng tên miền ".vn"

Theo Điều 9 Nghị định số 147/2024/NĐ-CP[2] thì Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) (Trung tâm Internet Việt Nam) quản lý tên miền quốc gia Việt Nam ".vn" và tên miền quốc tế mà tổ chức quốc tế phân bổ, cấp cho các cơ quan, tổ chức, doanh nghiệp, cá nhân tại Việt Nam.

- Các cơ quan, tổ chức, doanh nghiệp, cá nhân đều có quyền đăng ký tên miền quốc gia Việt Nam ".vn".
- Việc đăng ký, thay đổi thông tin đăng ký, hoàn trả tên miền quốc gia Việt Nam ".vn" thực hiện thông qua Nhà đăng ký tên miền quốc gia Việt Nam ".vn". Cơ quan, tổ chức, doanh nghiệp, cá nhân hoàn tất việc nộp lệ phí đăng ký sử dụng tên miền quốc gia Việt Nam ".vn" và phí duy trì sử dụng tên miền quốc gia Việt Nam ".vn" theo quy định trước khi tên miền được cấp quyền sử dụng hoặc được tiếp tục duy trì quyền sử dụng và trả tiền dịch vụ đăng ký, duy trì tên miền được cung cấp bởi các Nhà đăng ký tên miền quốc gia Việt Nam ".vn" theo thỏa thuận giữa hai bên.

(1) Nguyên tắc đăng ký tên miền ".vn":

Việc đăng ký tên miền quốc gia Việt Nam ".vn" thực hiện theo các nguyên tắc sau đây:

- Bình đẳng, không phân biệt đối xử.
- Đăng ký trước được xét cấp trước, trừ các tên miền được dành cho đấu giá theo quy định của pháp luật, tên miền được bảo vệ, tên miền dùng chung theo quy định.
- Tuân thủ quy định về đấu giá, chuyển nhượng quyền sử dụng tên miền theo quy định của Luật Viễn thông 2023[3] và các văn bản pháp luật có liên quan.

(2) Tên miền do cơ quan, tổ chức, doanh nghiệp, cá nhân đăng ký phải đảm bảo:

- Không có cụm từ xâm phạm đến lợi ích quốc gia.
- Phải phù hợp với đạo đức xã hội, thuần phong mỹ tục của dân tộc.
- Phải thể hiện tính nghiêm túc để tránh sự hiểu nhầm hoặc xuyên tạc do tính đa âm, đa nghĩa hoặc khi không dùng dấu trong tiếng Việt.
- Không được giống hoặc trùng với tên cơ quan báo chí, không có các cụm từ dễ gây nhầm lẫn là cơ quan báo chí hoặc sản phẩm báo chí nếu chủ thể đăng ký sử dụng không phải là cơ quan báo chí.
- Không có các cụm từ dễ gây nhầm lẫn là trang thông tin điện tử tổng hợp, mạng xã hội nếu chủ thể đăng ký sử dụng không phải đối tượng đăng ký tên miền để thiết lập trang thông tin điện tử tổng hợp, mạng xã hội theo quy định của pháp luật.

Lưu ý: *Tên miền là tên gọi các tổ chức của Đảng, cơ quan Nhà nước, tổ chức chính trị - xã hội chỉ dành cho các tổ chức của Đảng, cơ quan Nhà nước, tổ chức chính trị - xã hội; tổ chức, doanh nghiệp, cá nhân khác không được đăng ký, sử dụng các tên miền này.*

[2] Nghị định 147/2024/NĐ-CP (https://vanban.chinhphu.vn/?pageid=27160&docid=211654)
[3] Luật Viễn thông 2023 (https://vanban.chinhphu.vn/?pageid=27160&docid=209631&classid=1&typegroupid=3)

(3) Thông tin phải cung cấp khi đăng ký sử dụng tên miền:

- Đối với cơ quan, tổ chức, doanh nghiệp: Tên cơ quan, tổ chức, doanh nghiệp; mà định danh điện tử của tổ chức; mã số doanh nghiệp; mã số thuế; địa chỉ đầy đủ của trụ sở chính; số điện thoại; địa chỉ thư điện tử; thông tin người quản lý tên miền; thông tin người quản lý kỹ thuật của tên miền; thông tin tổ chức hoặc cá nhân nộp phí, lệ phí đăng ký sử dụng tên miền; mục đích sử dụng tên miền trong trường hợp đăng ký tên miền để thiết lập trang thông điện tử tổng hợp, mạng xã hội, báo điện tử và cập nhật thông tin mục đích sử dụng tên miền khi có thay đổi;
- Đối với cá nhân, hộ kinh doanh: Họ và tên cá nhân; tên hộ kinh doanh, họ và tên chủ hộ kinh doanh hoặc đại diện hộ kinh doanh; ngày, tháng, năm sinh; số định danh cá nhân hoặc số căn cước công dân hoặc số hộ chiếu và nơi cấp, ngày cấp; mã số đăng ký hộ kinh doanh; mã số thuế hộ kinh doanh; địa chỉ thường trú đầy đủ tới số nhà; địa chỉ tạm trú đầy đủ tới số nhà; số điện thoại; địa chỉ thư điện tử.

Lưu ý: *Chủ thể nộp hồ sơ đăng ký sử dụng tên miền được xác thực thông qua chữ ký số trong hồ sơ đăng ký tên miền, qua hệ thống định danh và xác thực điện tử hoặc giải pháp công nghệ để thu thập, kiểm tra, đối chiếu nhằm đảm bảo sự đầy đủ, khớp đúng giữa thông tin nhận biết chủ thể và thông tin, dữ liệu trên hồ sơ đăng ký sử dụng.*

- Công dân Việt Nam từ đủ 18 tuổi đến đủ 23 tuổi được ưu tiên, hỗ trợ trong đăng ký sử dụng tên miền cấp 3 dưới ".id.vn" bao gồm: miễn, giảm lệ phí đăng ký sử dụng tên miền quốc gia Việt Nam ".vn"; miễn, giảm phí duy trì sử dụng tên miền quốc gia Việt Nam ".vn" trong thời hạn cụ thể theo quy định của pháp luật về phí, lệ phí. Doanh nghiệp và Hộ kinh doanh có giấy chứng nhận đăng ký hộ kinh doanh theo quy định của pháp luật được ưu tiên, hỗ trợ trong đăng ký sử dụng tên miền cấp 3 dưới ".biz.vn" bao gồm: miễn, giảm về lệ phí đăng ký sử dụng tên miền quốc gia Việt Nam ".vn"; miễn, giảm phí duy trì sử dụng tên miền quốc gia Việt Nam ".vn" trong thời hạn cụ thể theo quy định của pháp luật về phí, lệ phí.
- Cơ quan, tổ chức, doanh nghiệp chỉ được sử dụng tên miền dưới tên miền đã đăng ký cho các đơn vị thành viên, cá nhân đang làm việc trong cơ quan, tổ chức trực thuộc và phải có trách nhiệm quản lý các tên miền cấp dưới tên miền đó. Cơ quan, tổ chức, doanh nghiệp, cá nhân không được cấp tên miền dưới tên miền của mình cho các chủ thể khác.
- Báo điện tử, mạng xã hội, trang thông tin điện tử tổng hợp, trang thông tin điện tử hoặc Cổng thông tin điện tử của các tổ chức của Đảng, cơ quan của Nhà nước phải sử dụng ít nhất 01 tên miền quốc gia Việt Nam ".vn" và lưu giữ thông tin tại hệ thống máy chủ có địa chỉ Internet ở Việt Nam.

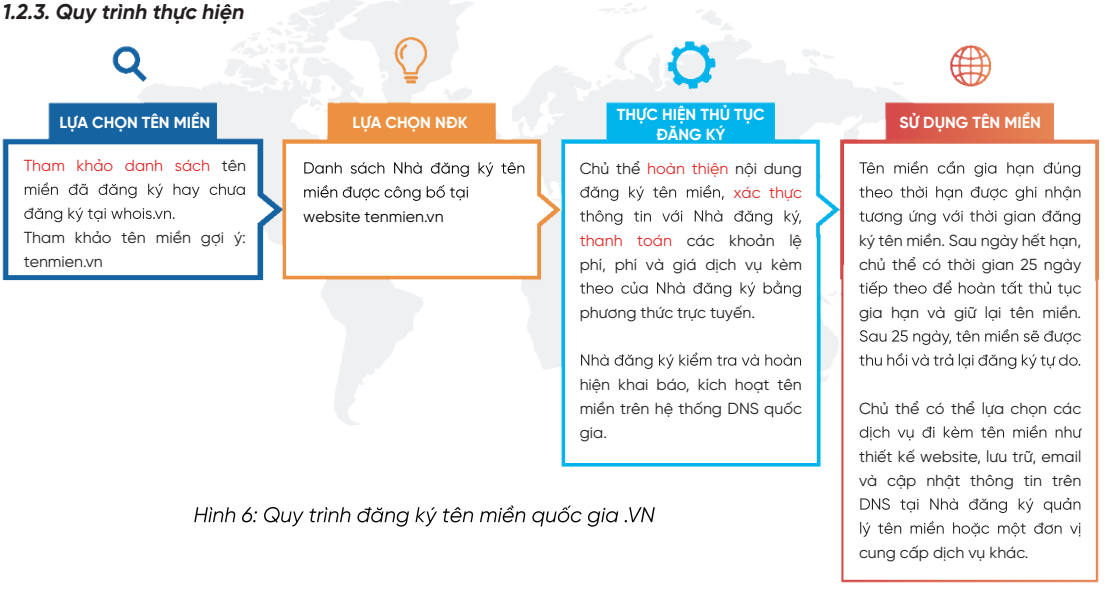
1.2.2. Giới thiệu về tên miền tiếng Việt (TMTV)

Tên miền tiếng Việt (TMTV) nằm trong hệ thống tên miền quốc gia Việt Nam ".vn", thuộc hệ thống tên miền đa ngữ IDN (Internationalized Domain Names) đã được quốc tế công nhận, trong đó các ký tự tạo nên tên miền là các ký tự được quy định trong bảng mã tiếng Việt theo tiêu chuẩn TCVN 6909:2001 và các ký tự nằm trong bảng mã mở rộng của tiếng Việt theo tiêu chuẩn trên. Việc đăng ký, sử dụng tên miền tiếng Việt bổ sung thêm nhiều lựa chọn, thay thế cho địa chỉ Website truyền thống chỉ chấp nhận những ký tự Latin thông thường.

Tên miền tiếng Việt được phát triển theo cấu trúc tên miền cấp 2 (trực tiếp sau ".vn"), không phát triển tên miền tiếng Việt dưới các đuôi tên miền cấp 2 dùng chung như .com.vn, .net.vn, ...

Ví dụ: thủđô.vn, chínhphủ.vn, ngườibạnsố.vn,...

1.2.3. Quy trình thực hiện



Hình 6: Quy trình đăng ký tên miền quốc gia .VN

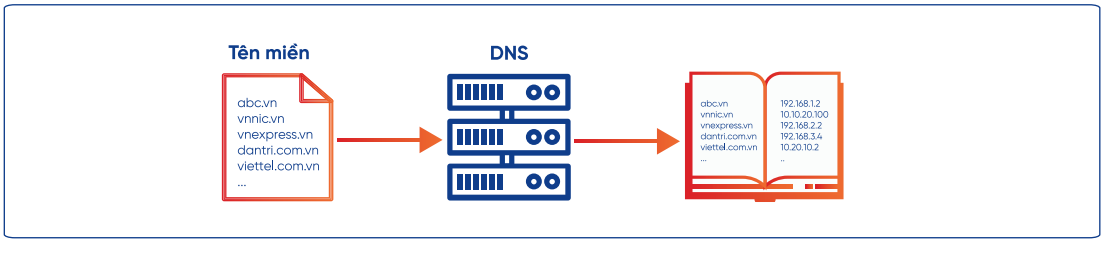
Chi tiết như sau:

STT	CÁC BƯỚC THỰC HIỆN	TRÁCH NHIỆM	MÔ TẢ	TÀI LIỆU, BIỂU MẪU
1	Chọn lựa tên miền	Chủ thể	- Chủ thể thực hiện kiểm tra sự tồn tại của tên miền dự định đăng ký thông qua WHOIS. - Lựa chọn tên miền ".vn" theo nguyên tắc đăng ký được quy định tại Điều 6 Thông tư số 24/2015/TT-BTTTT, sửa đổi, bổ sung tại điểm a, b khoản 6 Điều 1 Thông tư số 21/2021/TT-BTTTT.	- Thông tư số 24/2015/TT-BTTTT - Thông tư số 21/2021/TT-BTTTT
2	Chọn lựa Nhà đăng ký tên miền	Chủ thể	Chủ thể muốn đăng ký tên miền phải liên hệ với các nhà đăng ký tên miền của VNNIC. Danh sách Nhà đăng ký được công bố tại: http://nhadangky.vn (Lưu ý: Chủ thể có địa chỉ tại Việt Nam chỉ được nộp hồ sơ đăng ký tên miền tại NĐK tên miền ".vn" trong nước. Chủ thể có địa chỉ tại nước ngoài được đăng ký nộp hồ sơ đăng ký tên miền tại NĐK tên miền ".vn" trong nước và NĐK tên miền ".vn" nước ngoài.)	
3	Thực hiện thủ tục đăng ký tên miền	- Chủ thể - Nhà đăng ký	Chủ thể hoàn thiện hồ sơ đăng ký tên miền theo hướng dẫn của NĐK, bao gồm: (1) Bản khai đăng ký tên miền theo mẫu quy định của NĐK đã lựa chọn, nhưng phải đáp ứng đầy đủ các thông tin được quy định tại Phụ lục 3 Thông tư số 21/2021/TT-BTTTT. (2) Giấy tờ tùy thân: Giấy CMND/CCCD (hoặc hộ chiếu đối với người nước ngoài) của chủ thể là cá nhân; Giấy tờ tùy thân là bản gốc để NĐK đối chiếu với thông tin trong bản khai và bản có công chứng nếu gửi qua đường bưu chính tới địa chỉ của NĐK. (3) NĐK thực hiện việc đăng ký tên miền và tên miền sẽ được khai báo kích hoạt.	Phụ lục 3 Thông tư số 21/2021/TT-BTTTT
4	Sử dụng tên miền	- Chủ thể - Nhà đăng ký	Để đưa tên miền vào hoạt động, chủ thể liên hệ với NĐK để được hướng dẫn về các dịch vụ giá trị gia tăng trên tên miền (như khai báo tên miền – DNS hosting, cài đặt thông số Website,...).	

1.3. Tên miền gắn với DNS

Như đã đề cập trước đó, để một tên miền có thể hoạt động trên Internet và kết nối đến các dịch vụ trực tuyến, chúng ta cần phải khai báo các bản ghi tài nguyên tên miền, mà mỗi bản ghi này sẽ gắn với một dịch vụ cụ thể như Website, FTP, Mail,... Để hình dung dễ dàng hơn, chúng ta có thể coi tên miền giống như "tên của cá nhân" trong danh bạ số điện thoại. Tuy nhiên, chỉ có tên miền thôi thì vẫn chưa đủ để người dùng có thể xác định chính xác thông tin địa chỉ để truy cập vào các dịch vụ này một cách chính xác.

Để việc truy cập và tìm kiếm các dịch vụ trên Internet được diễn ra thuận lợi, chúng ta cần một hệ thống dẫn đường chính xác, giúp kết nối tên miền với các địa chỉ thực tế (địa chỉ IP) của các máy chủ lưu trữ các dịch vụ đó. Và hệ thống dẫn đường này chính là DNS (Domain Name System). Có thể tưởng tượng DNS giống như một cuốn danh bạ điện thoại, nơi tra cứu "tên của cá nhân" (tên miền) và tìm ra "số điện thoại" (địa chỉ IP) tương ứng. DNS không chỉ là một hệ thống kỹ thuật thông thường mà DNS chính là một hạ tầng hệ thống cốt lõi hay còn được gọi là "sổ địa chỉ" của Internet và đóng vai trò thiết yếu trong việc đảm bảo rằng khi người dùng nhập tên miền vào trình duyệt hay ứng dụng, người dùng sẽ được dẫn đến đúng địa chỉ và dịch vụ mà người dùng yêu cầu.



Hình 7: Tên miền và DNS

Tên miền và DNS là hai yếu tố không thể tách rời trong việc xây dựng và duy trì một hệ thống trực tuyến hoạt động hiệu quả. Nếu thiếu DNS, tên miền sẽ trở nên vô nghĩa vì không thể dẫn người dùng đến đúng nơi cần thiết. Mối quan hệ giữa chúng giống như việc có một cuốn sổ địa chỉ (tên miền) nhưng không có một bản đồ (DNS) để chỉ dẫn, từ đó khiến cho việc tìm kiếm và kết nối các dịch vụ trở nên khó khăn và không hiệu quả.

2. Quản lý, đăng ký sử dụng địa chỉ IP, số hiệu mạng

2.1. Nguyên tắc thực hiện chung

2.1.1. Đối tượng được đề nghị phân bổ, cấp địa chỉ Internet

- Cơ quan, tổ chức, doanh nghiệp có nhu cầu thiết lập mạng kết nối với Internet được quyền đề nghị phân bổ, cấp địa chỉ Internet để sử dụng nội bộ hoặc cấp lại cho khách hàng trong trường hợp cung cấp dịch vụ viễn thông.
- Cơ quan, tổ chức, doanh nghiệp có nhu cầu được phân bổ, cấp địa chỉ Internet IPv4 từ vùng địa chỉ Internet IPv4 sau hoàn trả hoặc thu hồi đã được Bộ Thông tin và Truyền thông[4] (Trung tâm Internet Việt Nam) niêm yết.
- Cơ quan, tổ chức, doanh nghiệp thay đổi tên chủ thể đăng ký trong các trường hợp quy định tại khoản 5 Điều 17, Nghị định số 147/2024/NĐ-CP.
- Cơ quan, tổ chức, doanh nghiệp nhận địa chỉ Internet hoặc số hiệu mạng từ các tổ chức quốc tế.

2.1.2. Nguyên tắc phân bổ, cấp địa chỉ Internet và số hiệu mạng

a. Đăng ký trước, được xét phân bổ, cấp trước.
b. Việc phân bổ, cấp địa chỉ Internet và số hiệu mạng đồng bộ với chính sách phân bổ, cấp địa chỉ Internet và số hiệu mạng quy định bởi tổ chức quản lý địa chỉ khu vực châu Á - Thái Bình Dương (APNIC).
c. Địa chỉ Internet thu hồi hoặc được hoàn trả từ các cơ quan, tổ chức, doanh nghiệp được phân bổ, cấp theo nguyên tắc đăng ký trước được xét duyệt xử lý hồ sơ trước và căn cứ trên mức độ cần thiết, khả năng sử dụng ngay vùng địa chỉ đề nghị phân bổ, cấp thể hiện qua việc cơ quan, tổ chức, doanh nghiệp chưa có địa chỉ Internet để sử dụng hoặc đã sử dụng hết ít nhất 80% các vùng địa chỉ Internet được phân bổ, cấp trước đó.
. Bộ Khoa học và Công nghệ (Trung tâm Internet Việt Nam) niêm yết thông tin về vùng địa chỉ Internet và thời điểm mở tiếp nhận hồ sơ đề nghị phân bổ, cấp lại vùng địa chỉ Internet tại địa chỉ diachiip.vn.
d. Cơ quan, tổ chức, doanh nghiệp Việt Nam nhận địa chỉ Internet và số hiệu mạng từ các tổ chức quốc tế phải báo cáo với Bộ Khoa học và Công nghệ (Trung tâm Internet Việt Nam) để đưa vùng địa chỉ Internet hoặc số hiệu mạng vào danh mục quản lý bởi Bộ Khoa học và Công nghệ. Địa chỉ Internet, số hiệu mạng tiếp nhận vào Việt Nam theo quy định sẽ là tài nguyên Internet Việt Nam, được Bộ Khoa học và Công nghệ phân bổ, cấp.

2.1.3. Đăng ký số hiệu mạng

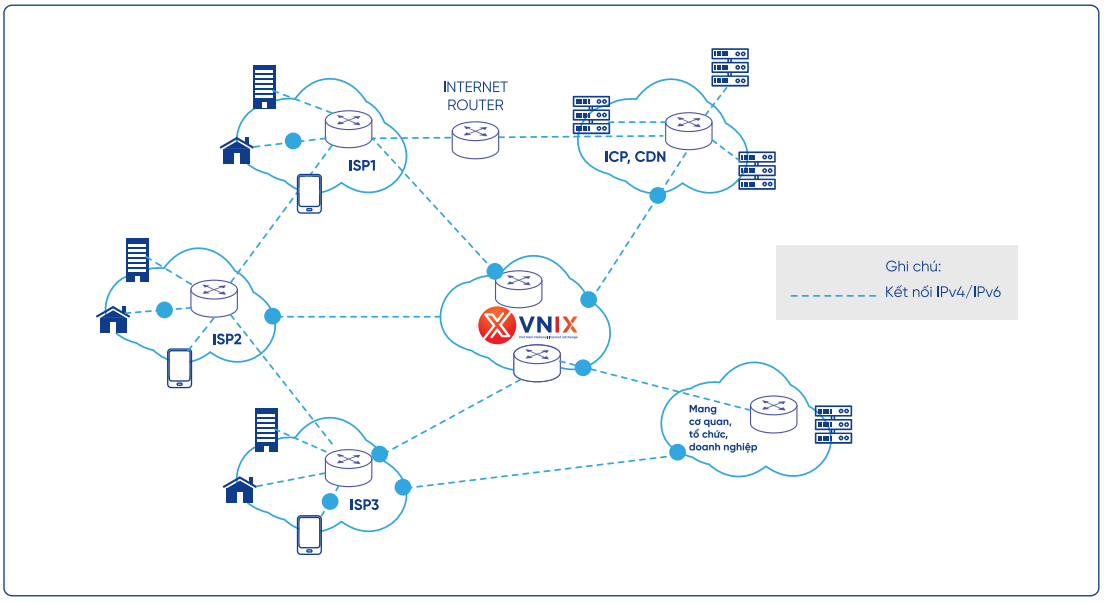
Các cơ quan, tổ chức, doanh nghiệp đã được phân bổ, cấp địa chỉ Internet thì được đăng ký sử dụng số hiệu mạng. Bộ Khoa học và Công nghệ sử dụng hồ sơ và thông tin mà cơ quan, tổ chức, doanh nghiệp đã nộp khi đăng ký địa chỉ Internet để cấp số hiệu mạng khi cơ quan, tổ chức, doanh nghiệp có yêu cầu.

2.1.4. Khuyến khích đăng ký, sử dụng IPv6; kết nối BGP Multihome, đa hướng với nhiều nhà cung cấp dịch vụ Internet; kết nối VNIX

- Khuyến khích việc đăng ký sử dụng địa chỉ IPv6.
- Địa chỉ IP, ASN được cấp, phân bổ cho nhu cầu sử dụng thực tế và có giá trị sử dụng trên toàn bộ lãnh thổ Việt Nam. Các cơ quan, tổ chức, doanh nghiệp tham gia hoạt động Internet phải đảm bảo:

+ Thực hiện việc định tuyến các vùng địa chỉ IP ở Việt Nam theo hướng dẫn của Bộ Khoa học và Công nghệ (VNNIC).
+ Không được định tuyến những vùng địa chỉ IP nằm ngoài danh mục quản lý của Bộ Khoa học và Công nghệ (VNNIC) trừ trường hợp kết nối với cổng quốc tế.
+ Phối hợp với VNNIC về kỹ thuật và chính sách định tuyến để đảm bảo hệ thống DNS quốc gia và trạm trung chuyển Internet quốc gia (VNIX), Internet Việt Nam hoạt động an toàn, hiệu quả.
+ Có kế hoạch đưa địa chỉ IPv6 đi vào hoạt động phù hợp kế hoạch hành động quốc gia về IPv6.

[4] Bộ Thông tin và Truyền thông nay là Bộ Khoa học và Công nghệ



Hình 8: Mô hình mạng hiện đại, kết nối đa hướng BGP Multihome

2.1.5. Trường hợp đổi tên chủ thể đăng ký sử dụng địa chỉ IP, ASN

Cơ quan, tổ chức, doanh nghiệp được đề nghị thay đổi tên chủ thể đăng ký sử dụng địa chỉ Internet, số hiệu mạng trong các trường hợp sau:

- Cơ quan, tổ chức, doanh nghiệp đổi tên theo quyết định của cấp có thẩm quyền.
- Chia, tách, sáp nhập, hợp nhất hoặc thay đổi chức năng nhiệm vụ của cơ quan, tổ chức, doanh nghiệp theo quyết định của cơ quan nhà nước có thẩm quyền, dẫn tới sự thay đổi về tổ chức quản lý, vận hành mạng, dịch vụ đang sử dụng vùng địa chỉ Internet, số hiệu mạng.
- Tổ chức lại doanh nghiệp theo quy định của Luật Doanh nghiệp hoặc có hoạt động mua bán doanh nghiệp, góp vốn, cổ phần giữa các doanh nghiệp hoặc chuyển đổi chức năng, nhiệm vụ giữa nhóm công ty, công ty mẹ, công ty con dẫn tới sự thay đổi về tổ chức trực tiếp quản lý, vận hành mạng, dịch vụ đang sử dụng vùng địa chỉ Internet, số hiệu mạng.

2.1.6. Nhận địa chỉ IP, ASN trực từ các tổ chức quốc tế

Các cơ quan, tổ chức, doanh nghiệp ở Việt Nam nhận địa chỉ Internet, số hiệu mạng từ các tổ chức quốc tế phải thực hiện:

- Đóng các khoản phí phát sinh theo quy định của các tổ chức quản lý địa chỉ quốc tế để có thể thực hiện chuyển vùng địa chỉ, số hiệu mạng vào danh mục quản lý của Bộ Khoa học và Công nghệ (Trung tâm Internet Việt Nam).
- Nộp lệ phí phân bổ, cấp tài nguyên Internet và phí duy trì sử dụng tài nguyên Internet theo quy định của pháp luật về phí và lệ phí.

2.1.7. Thu hồi địa chỉ IP, ASN trong các trường hợp

- Theo Quyết định của Bộ trưởng Bộ Thông tin và Truyền thông đối với các trường hợp thu hồi địa chỉ Internet, số hiệu mạng phục vụ lợi ích quốc gia, lợi ích công cộng, phát triển kinh tế - xã hội, quốc phòng, an ninh hoặc không còn phù hợp quy hoạch tài nguyên Internet quy định tại Luật Viễn thông.
- Theo quyết định xử phạt vi phạm hành chính của thanh tra chuyên ngành thông tin và truyền thông có áp dụng biện pháp khắc phục hậu quả là thu hồi địa chỉ Internet, số hiệu mạng hoặc áp dụng hình thức xử phạt bổ sung tịch thu phương tiện vi phạm.
- Theo yêu cầu bằng văn bản của cơ quan điều tra hoặc cơ quan nhà nước có thẩm quyền theo quy định của pháp luật về an ninh mạng và phòng, chống tội phạm công nghệ cao để ngăn chặn các hành vi sử dụng địa chỉ Internet, số hiệu mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội theo quy định của pháp luật.
- Địa chỉ Internet, số hiệu mạng không nộp đủ phí duy trì sử dụng trong thời hạn 30 ngày kể từ ngày đến hạn nộp phí.
- Các trường hợp thông tin đăng ký sử dụng địa chỉ Internet, số hiệu mạng không chính xác hoặc không xác định được chủ thể đăng ký sử dụng địa chỉ Internet, số hiệu mạng do chủ thể không cập nhật, bổ sung hoặc hoàn thiện thông tin.

2.2. Thành phần hồ sơ cấp, phân bổ địa chỉ IP, ASN

2.2.1. Thành phần hồ sơ khi đăng ký mới địa chỉ IP (hoặc IP và ASN)

- Bản khai đăng ký địa chỉ IP (hoặc IP và ASN).
- Bản sao hợp lệ (bao gồm bản sao được cấp từ sổ gốc hoặc bản sao chứng thực hoặc bản sao chứng thực điện tử hoặc bản sao đối chiếu với bản gốc) Quyết định thành lập, hoặc bản sao hợp lệ giấy chứng nhận, giấy phép tương đương hợp lệ khác được cấp trước ngày có hiệu lực của Luật Đầu tư số 67/2014/QH13 và Luật Doanh nghiệp số 59/2020/QH14.

2.2.2. Thành phần hồ sơ khi đề nghị đổi tên chủ thể đăng ký sử dụng địa chỉ IP (hoặc IP và ASN)

- Bản khai đăng ký địa chỉ IP (hoặc IP và ASN).
- Bản sao hợp lệ (bao gồm bản sao được cấp từ sổ gốc hoặc bản sao chứng thực hoặc bản sao chứng thực điện tử hoặc bản sao đối chiếu với bản gốc) Quyết định thành lập, hoặc bản sao hợp lệ giấy chứng nhận, giấy phép tương đương hợp lệ khác được cấp trước ngày có hiệu lực của Luật Đầu tư số 67/2014/QH13 và Luật Doanh nghiệp số 59/2020/QH14.
- Bản sao hợp lệ quyết định của cơ quan nhà nước có thẩm quyền hoặc văn bản tổ chức lại doanh nghiệp theo quy định của Luật Doanh nghiệp và các giấy tờ chứng minh sự thay đổi hợp lệ về quyền sử dụng.

2.2.3. Thành phần hồ sơ trong trường hợp đăng ký tái cấp địa chỉ IPv4

- Bản khai đăng ký địa chỉ [5].
- Bản sao hợp lệ (bao gồm bản sao được cấp từ sổ gốc hoặc bản sao chứng thực hoặc bản sao chứng thực điện tử hoặc bản sao đối chiếu với bản gốc) Quyết định thành lập, hoặc bản sao hợp lệ giấy chứng nhận, giấy phép tương đương hợp lệ khác được cấp trước ngày có hiệu lực của Luật Đầu tư số 67/2014/QH13 và Luật Doanh nghiệp số 59/2020/QH14.
- Báo cáo sử dụng vùng địa chỉ đã được cấp và kế hoạch sử dụng vùng địa chỉ có nhu cầu đăng ký.

2.2.4. Thành phần hồ sơ trong trường hợp nhận địa chỉ IP/ASN từ tổ chức quốc tế

- Bản khai đăng ký địa chỉ IP (hoặc IP và ASN) [6].
- Bản sao hợp lệ (bao gồm bản sao được cấp từ sổ gốc hoặc bản sao chứng thực hoặc bản sao chứng thực điện tử hoặc bản sao đối chiếu với bản gốc) Quyết định thành lập, hoặc bản sao hợp lệ giấy chứng nhận, giấy phép tương đương hợp lệ khác được cấp trước ngày có hiệu lực của Luật Đầu tư số 67/2014/QH13 và Luật Doanh nghiệp số 59/2020/QH14.
- Báo cáo sử dụng vùng địa chỉ đã được cấp và kế hoạch sử dụng vùng địa chỉ có nhu cầu đăng ký.

2.3. Phương thức nộp hồ sơ

a) Nộp trực tuyến tại địa chỉ: https://dichvucong.mst.gov.vn; hoặc https://dichvucong.gov.vn/.

b) Trường hợp không thể nộp trực tuyến thì nộp trực tiếp hoặc qua bưu chính tới địa chỉ: Trung tâm Internet Việt Nam, tòa nhà VNTA, tầng 24, Dương Đình Nghệ, Yên Hòa, Cầu Giấy, Hà Nội.

2.4. Quy trình thực hiện

(1) Cơ quan, tổ chức, doanh nghiệp nộp 01 bộ hồ sơ trực tiếp hoặc thông qua dịch vụ bưu chính hoặc nộp trực tuyến tới Bộ Thông tin và Truyền thông (Trung tâm Internet Việt Nam).

Trường hợp nộp trực tuyến, phải có chữ ký số theo quy định của pháp luật về giao dịch điện tử.

(2) Trung tâm Internet Việt Nam tiếp nhận và giải quyết hồ sơ theo quy định.

(3) Trung tâm Internet Việt Nam thông báo về thu phí, lệ phí đăng ký địa chỉ IP, ASN cho cơ quan, tổ chức, doanh nghiệp (nếu có).

(4) Cơ quan, tổ chức, doanh nghiệp hoàn tất nộp phí, lệ phí.

(5) Trung Internet Việt Nam xử lý thủ tục cấp, phân bổ địa chỉ IP (hoặc IP và ASN).

(6) Trả kết quả: Trong thời hạn 10 ngày kể từ ngày nhận được hồ sơ, lệ phí đăng ký sử dụng địa chỉ Internet, số hiệu mạng; phí duy trì sử dụng địa chỉ Internet, số hiệu mạng đầy đủ, hợp lệ, Bộ Khoa học và công nghệ (Trung tâm Internet Việt Nam) có trách nhiệm phân bổ, cấp địa chỉ Internet, số hiệu mạng cho cơ quan, tổ chức, doanh nghiệp.

Trường hợp từ chối phân bổ, cấp, Bộ Khoa học và Công nghệ (Trung tâm Internet Việt Nam) phải thông báo kết quả bằng văn bản và nêu rõ lý do.

[5] https://vnnic.vn/sites/default/files/mau-2025-ban_khai_dang_ky_cap_ip_hoac_ip_va_asn_0.docx
[6] https://vnnic.vn/sites/default/files/mau-2022-ban_khai_dang_ky_cap_ip_hoac_ip_va_asn.docx

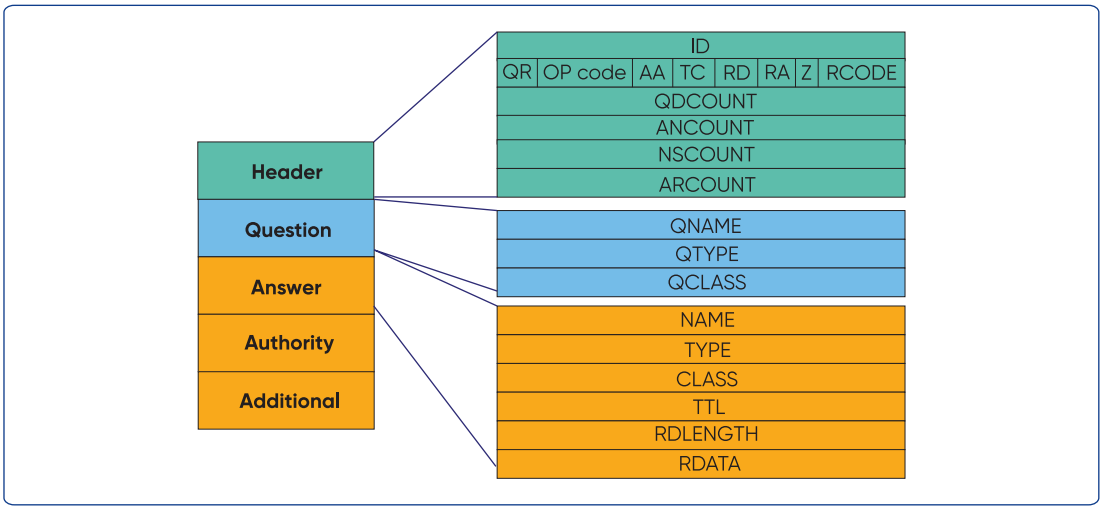
IV

GIAO THỨC DNS

Giao thức DNS (Domain Name System) sử dụng các gói tin (messages) để trao đổi dữ liệu giữa các máy khách (clients) và máy chủ DNS. Các gói tin này có cấu trúc rõ ràng và được sử dụng để truy vấn và trả lời các truy vấn DNS. Một gói tin DNS bao gồm nhiều phần, từ header cho đến các câu hỏi (truy vấn), câu trả lời, trường thông tin bổ sung và các bản ghi Authority. Để hiểu sâu hơn về giao thức DNS, chúng ta sẽ phân tích hai phần quan trọng của nó: Format và Transport.

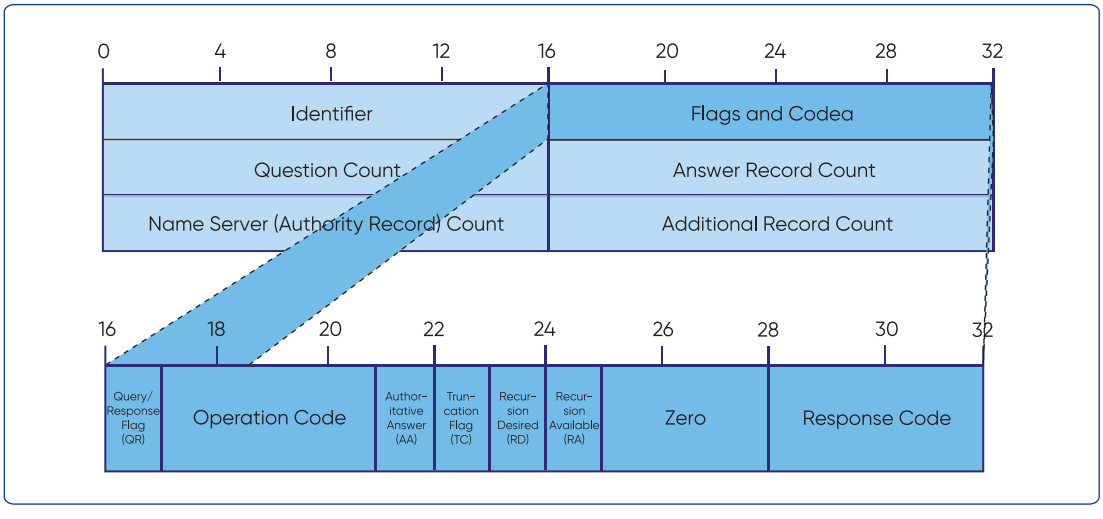
1. Định dạng (Format)

Gói tin DNS được phân thành 2 loại: truy vấn (query message) và phản hồi (response message), cả hai loại đều có định dạng, cấu trúc giống nhau như sau:



Hình 9: Cấu trúc gói tin DNS

1.1. Header



Hình 10: Định dạng header của gói tin DNS

Tiêu đề (header) là mô tả loại gói tin và trường nào được chứa trong gói tin đó. Phần Header bao gồm những thông tin chi tiết sau:

- ID (Identification): Mã định danh 16 bit được tạo ngẫu nhiên. Mã định danh này giống với mã nhận dạng khi nhận được phản hồi từ máy chủ DNS.
- Flags (Cờ): 16 bit, bao gồm các cờ sau:

+ QR (Query/Response): Trường 01 bit chỉ định xem gói tin này là truy vấn (0) hay phản hồi (1).
+ OPCODE : Trường 04 bit, xác định loại truy vấn DNS, bao gồm các loại:

GIÁ TRỊ OPCODE	LOẠI TRUY VẤN/	MÔ TẢ
0	QUERY	Truy vấn chuẩn, thông thường.
1	IQUERY	Truy vấn ngược. Tuy nhiên, theo RFC 3425, phương thức này đã lỗi thời và không còn được khuyến nghị sử dụng.
2	STATUS	Truy vấn được sử dụng để kiểm tra tình trạng của máy chủ DNS.
3	NSID Request	Đây là một truy vấn đặc biệt để lấy NSID (DNS Server Identifier), tức là một định danh duy nhất của một máy chủ tên miền (được mô tả trong RFC 5001).
4	NOTIFY	Các bản tin thông báo Notify.
5	DDNS update	Cập nhật DDNS.
6-15	Unused	Chưa sử dụng và sẵn sàng để phân bổ.

+ AA (Authoritative Answer – 01 bit): Đánh dấu là phản hồi Authoritative, bit này được đặt thành 1 trong phản hồi để chỉ ra rằng máy chủ DNS tạo ra phản hồi là máy chủ Authoritative đối với zone tên miền được chỉ định trong phần câu hỏi/truy vấn. Nếu giá trị là 0, phản hồi không phải là Authoritative.
+ TC (Truncated – 01 bit): Khi được đặt thành 1, điều này chỉ ra rằng gói tin DNS đã bị cắt ngắn vì chiều dài của nó vượt quá giới hạn tối đa cho cơ chế vận chuyển (UDP/TCP) được sử dụng. TCP không có giới hạn kích thước cho các gói tin, tuy nhiên các gói tin UDP bị giới hạn ở 512 byte, vì vậy bit này thường được gửi đi như một thông báo rằng gói tin đã được gửi qua UDP và kích thước gói tin quá lớn. Trong trường hợp này giữa client và DNS server cần thiết lập một phiên TCP để nhận gói tin đầy đủ.
+ RD (Recursion Desired – 01 bit): Khi được đặt trong một truy vấn, yêu cầu máy chủ nhận truy vấn cố gắng trả lời truy vấn bằng truy vấn đệ quy, nếu máy chủ hỗ trợ phân giải đệ quy (recursive resolution). Giá trị của bit này không thay đổi trong phản hồi.
+ RA (Recursion Available): Được đặt thành 1 hoặc cleared (xóa) thành 0 trong phản hồi để chỉ ra liệu máy chủ DNS tạo ra phản hồi có hỗ trợ các truy vấn đệ quy hay không. Điều này có thể được ghi nhận bởi thiết bị gửi truy vấn để sử dụng trong tương lai.
+ Z (Zero – 03 bit): Các bit dự trữ để sử dụng trong tương lai (được đặt thành 0).

- RCODE (Response Code – 04 bit): Mã phản hồi - được đặt thành zero (0) trong các truy vấn, sau đó thay đổi bởi máy chủ DNS phản hồi để truyền tải kết quả của việc xử lý truy vấn. Trường này dùng để chỉ ra liệu truy vấn có được trả lời thành công hay không, hoặc nếu có lỗi xảy ra. Chi tiết các giá trị RCODE như sau:

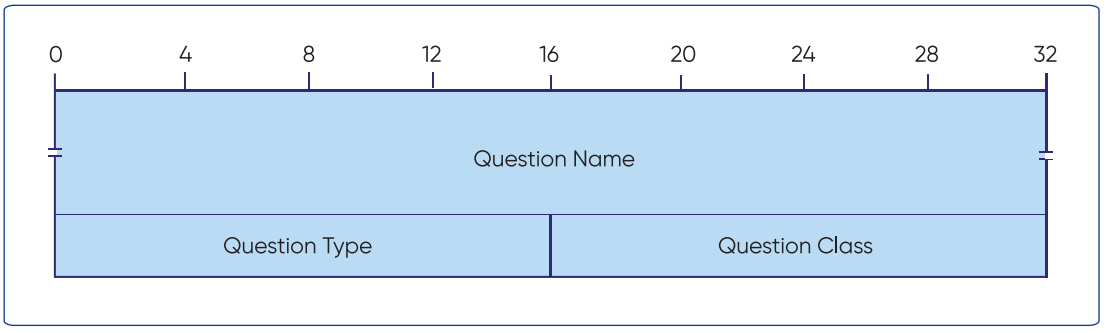
GIÁ TRỊ RCODE	MÃ PHẢN HỒI	MÔ TẢ
0	NOERROR	Không có lỗi xảy ra.
1	FORMERR	Lỗi định dạng - Máy chủ không thể thực hiện truy vấn do lỗi định dạng truy vấn.
2	SERVFAIL	Lỗi máy chủ - Máy chủ không thể phản hồi truy vấn do vấn đề với chính máy chủ đó.
3	NXDOMAIN	Lỗi tên miền - Tên được chỉ định trong truy vấn không tồn tại. Mã này thường chỉ phản hồi từ phía các máy chủ Authoritative DNS Server.
4	NOTIMP	Chưa triển khai - Máy chủ DNS không hỗ trợ loại truy vấn được yêu cầu.

GIÁ TRỊ RCODE	MÃ PHẢN HỒI	MÔ TẢ
5	REFUSED	Máy chủ từ chối xử lý truy vấn, thường là vì lý do chính sách, không phải lý do kỹ thuật.
6	YXDomain	Tên miền tồn tại khi không nên có (được mô tả trong RFC 2136).
7	YXRRSet	Bộ bản ghi (RR Set) tồn tại khi không nên có (được mô tả trong RFC 2136).
8	NXRRSet	Bộ bản ghi không tồn tại khi nó nên có (được mô tả trong RFC 2136).
9	NotAuth	Máy chủ không phải là Authoritative đối với zone tên miền (được mô tả trong RFC 2136).
10	NotZone	Tên miền không có trong zone (được mô tả trong RFC 2136).
11-15	Unused	Sẵn sàng để phân bổ. Giá trị mở rộng RCODE chỉ có thể sử dụng với EDNS0
16	BADVERS	Phiên bản OPT không hợp lệ (không phải OPT=0) (được mô tả trong RFC 2671).
16	BADSIG	Lỗi chữ ký TSIG (được mô tả trong RFC 2845).
17	BADKEY	Khóa không nhận dạng được (được mô tả trong RFC 2845). Thông thường trong các cấu hình TSIG và lỗi do đồng bộ thời gian
18	BADTIME	Chữ ký được gửi nằm ngoài khoảng thời gian hợp lệ (được mô tả trong RFC 2845).
19	BADMODE	Chế độ TKEY không hợp lệ (được mô tả trong RFC 2930).
20	BADNAME	Tên trùng lặp (được mô tả trong RFC 2930).
21	BADALG	Thuật toán không được hỗ trợ (được mô tả trong RFC 2930).
22-3840	Not used	Chưa sử dụng và sẵn sàng để phân bổ
3841-4095	Private use	Sử dụng cho mục đích riêng tư
4096-65535	Not used	Chưa sử dụng và sẵn sàng để phân bổ

- QDCOUNT (Question Count): Có định dạng là số nguyên với chiều dài 16 bit không dấu xác định số mục trong phần câu hỏi. Nếu trường này được thiết lập bằng 1, cho biết đây là một câu hỏi truy vấn.
- ANCOUNT (Answer Record Count): Có định dạng là số nguyên 16 bit không dấu chỉ định số lượng bản ghi tài nguyên trong phần câu trả lời. Nếu đặt trường này thành 0, đồng nghĩa với việc không có bất kỳ phản hồi truy vấn nào.
- NSCOUNT (Authority Record Count): Có định dạng là số nguyên 16 bit không dấu chỉ định số lượng bản ghi tài nguyên máy chủ tên miền trong phần bản ghi chuyển giao.
- ARCOUNT (Additional Record Count): Có định dạng là số nguyên 16 bit không dấu chỉ định số lượng bản ghi tài nguyên trong phần bản ghi bổ sung.

1.2. Định dạng phần câu hỏi (query/request)

Phần câu hỏi được sử dụng để chứa "câu hỏi" trong hầu hết các truy vấn, tức là các tham số xác định các thông tin đang được hỏi và chỉ được phép có một câu hỏi trong mỗi gói tin (được xác định bởi QDCOUNT như đã đề cập trước đó).



Hình 11: Định dạng phần câu hỏi

Trong đó:

- QNAME: là trường chứa tên miền mà người dùng yêu cầu phân giải. Đây là tên miền mà máy chủ DNS sẽ tìm kiếm và trả về thông tin liên quan (ví dụ, địa chỉ IP hoặc các bản ghi khác). Tên miền này được mã hóa theo định dạng DNS. Mỗi phần của tên miền (từng phần giữa dấu chấm – các nhãn tên miền) sẽ được ghi lại theo độ dài của phần đó và sau đó là chính phần tên.

Ví dụ:
Đối với tên miền "www.vnnic.vn", QNAME sẽ được mã hóa như sau:

- "www" sẽ được mã hóa là 3 ký tự (số 3 biểu thị độ dài của phần "www" và sau đó là chính phần "www").
- Tiếp theo là "vnnic" với độ dài là 5 và nội dung là "vnnic".
- Cuối cùng, "vn" sẽ có độ dài là 2 và nội dung là "vn".

Vì vậy, QNAME sẽ có định dạng là:

- 3 "www" + 5 "vnnic" + 2 "vn" = 3 www 5 vnnic 2 vn.

- QTYPE: là trường xác định loại bản ghi DNS mà người dùng muốn truy vấn. Các giá trị phổ biến của QTYPE bao gồm:

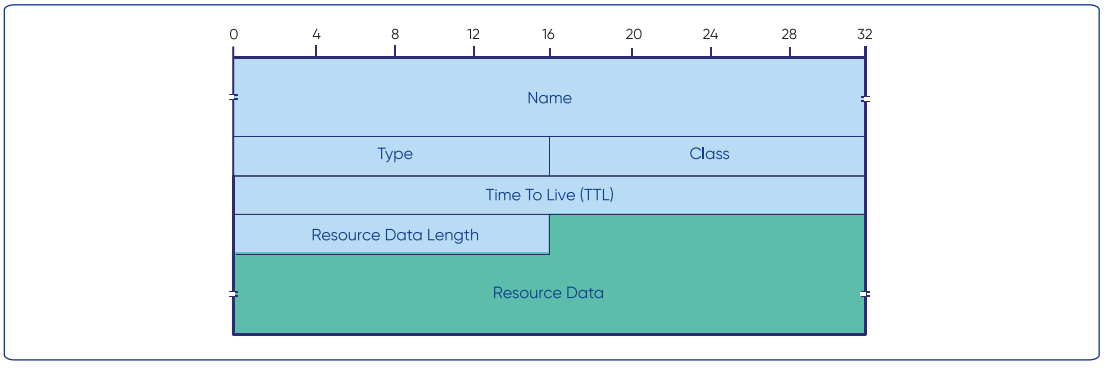
GIÁ TRỊ QTYPE	LOẠI BẢN GHI	MÔ TẢ
1	A	Truy vấn cho địa chỉ IPv4 của tên miền.
28	AAAA	Truy vấn cho địa chỉ IPv6 của tên miền.
15	MX	Truy vấn cho bản ghi Mail Exchange (MX), chỉ định máy chủ thư điện tử cho tên miền.
3	CNAME	Truy vấn cho bản ghi Canonical Name, cho phép một tên miền trỏ đến một tên miền khác.
2	NS	Truy vấn cho bản ghi DNS Server, chỉ định máy chủ DNS của tên miền.
12	PTR	Truy vấn cho bản ghi Pointer, thường được sử dụng trong truy vấn ngược để ánh xạ địa chỉ IP đến tên miền.
6	SOA	Truy vấn cho bản ghi Start of Authority, chỉ ra máy chủ chính thức cho một zone tên miền.
16	TXT	Truy vấn cho bản ghi Text, chứa dữ liệu văn bản tùy chỉnh.

- QCLASS: Xác định lớp của bản ghi DNS mà người dùng yêu cầu. Thông thường, lớp này được đặt là IN (Internet), có nghĩa là bản ghi DNS mà người dùng yêu cầu thuộc lớp Internet. Ngoài rà còn có các lớp khác ít gặp hơn như:

+ CH (Chaos): Một lớp đặc biệt cho các ứng dụng không phải Internet, chủ yếu được sử dụng trong môi trường thử nghiệm.
+ HS (Hesiod): Cũng là một lớp đặc biệt được sử dụng trong một số hệ thống phân tán.

1.3. Định dạng phần phản hồi (Response)

Các phần ANSWER, AUTHORITY, và ADDITIONAL chứa các bản ghi tài nguyên DNS (RR - Resource Record) và đều có cùng một định dạng. Phần mà bản ghi RR xuất hiện được xác định hoàn toàn bởi số lượng bản ghi trong mỗi phần, được chứa trong header của gói tin. Do đó, một bản ghi A có thể xuất hiện trong phần ANSWER hoặc ADDITIONAL. Mỗi bản ghi tài nguyên có định dạng như sau:



Hình 12: Định dạng phần phản hồi

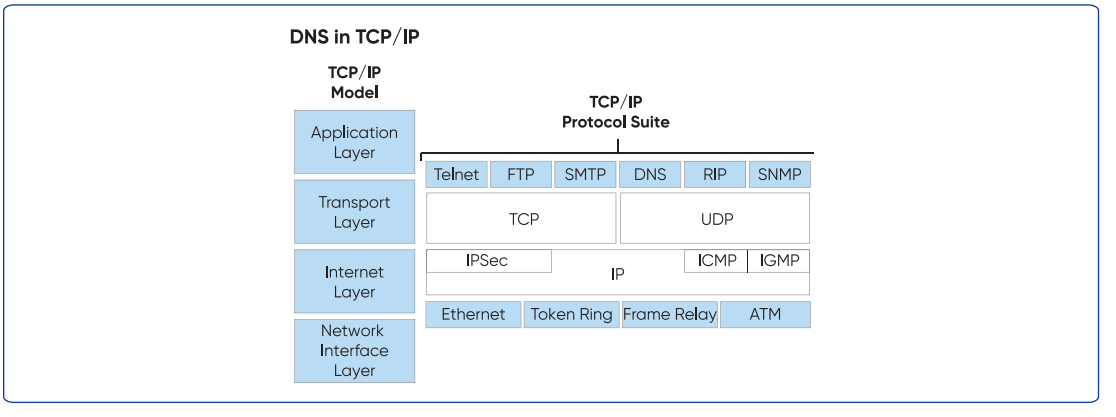
- NAME: Tên miền được truy vấn, có cùng định dạng với QNAME trong câu hỏi.
- TYPE: Xác định loại của bản ghi tài nguyên trong mỗi phần. Trường này xác định ý nghĩa của dữ liệu trong trường RDATA. Các giá trị phổ biến cho TYPE trong các phần như mô tả trong phần QTYPE.
- CLASS: Xác định lớp của bản ghi tài nguyên DNS. Lớp phổ biến nhất là IN (Internet), có nghĩa là bản ghi này dành cho mạng Internet.
- TTL: Giá trị thời gian Time-to-live (sẽ dùng để lưu và bộ nhớ đệm).
- RDLENGTH: Độ dài của trường RDATA.
- RDATA: Là trường chứa dữ liệu thực tế của bản ghi tài nguyên, dữ liệu này thay đổi tùy theo loại bản ghi (TYPE).

- A record: RDATA chứa địa chỉ IPv4 (ví dụ: 192.168.1.1).
- MX record: RDATA chứa địa chỉ máy chủ thư (mail server) và mức độ ưu tiên.
- CNAME record: RDATA chứa tên miền mà bản ghi CNAME trỏ đến.
- NS record: RDATA chứa tên của máy chủ Authoritative DNS Server của tên miền.

2. Truyền tải (Transport)

Truyền tải trong DNS là quá trình gửi và nhận các gói tin DNS giữa các trình giải phân giải DNS (DNS resolvers) và các máy chủ DNS. Hai tài liệu RFC quan trọng cho việc mô tả nguyên lý và các yêu cầu của truyền tải DNS là RFC 1033 và RFC 1034.

Hai giao thức truyền tải chính được sử dụng để truyền tải các gói tin DNS là UDP (User Datagram Protocol) và TCP (Transmission Control Protocol) và đều sử dụng cổng 53 (53/UDP và 53/TCP). Mỗi giao thức này có những đặc điểm riêng biệt, phục vụ các nhu cầu khác nhau trong quá trình truy vấn và phân giải tên miền.



Hình 13: Giao thức DNS trong mô hình TCP/IP

2.1. Truyền tải qua gói tin UDP

UDP là giao thức chủ yếu được sử dụng trong DNS, nhờ vào tính hiệu quả và tốc độ của nó. Với UDP, việc truyền tải các gói tin DNS diễn ra nhanh chóng, giúp giảm độ trễ và tài nguyên sử dụng khi xử lý các truy vấn có kích thước nhỏ. Đây là lý do chính khiến UDP trở thành lựa chọn chính cho các truy vấn DNS đơn giản, như yêu cầu phân giải tên miền sang địa chỉ IP. Tuy nhiên, UDP không cung cấp cơ chế đảm bảo độ tin cậy, nghĩa là các gói tin có thể bị mất mà không có thông báo lỗi. Do đó, kích thước gói tin DNS qua UDP được giới hạn ở 512 byte để đảm bảo tính ổn định và hiệu suất trong mạng. Nếu một gói tin DNS vượt quá giới hạn này, hệ thống DNS sẽ tự động chuyển sang TCP để đảm bảo dữ liệu không bị mất.

Lưu ý:
Giới hạn 512 byte đối với các gói tin DNS qua UDP có thể vượt qua, nếu áp dụng và hỗ trợ tiêu chuẩn mở rộng (EDNS0) trên các hệ thống máy chủ DNS (được mô tả trong RFC 2671).

2.2. Truyền tải qua gói tin TCP

Đối với một số truy vấn và phản hồi truy vấn DNS đặc biệt, việc truyền tải sử dụng qua UDP là không phù hợp (bị giới hạn bởi kích thước 512 byte như đã đề cập ở trên). Ví dụ như việc đồng bộ dữ liệu (zone transfer) giữa máy chủ DNS Primary và DNS Secondary. Mặc dụ gói tin truy vấn cho zone transfer có kích thước rất nhỏ, tuy nhiên gói tin được gửi trong phản hồi có thể có kích thước rất lớn. Đồng thời, việc đồng bộ dữ liệu zone transfer phải được thực hiện một cách an toàn và đáng tin cậy, nếu không sẽ có nguy cơ thông tin đồng bộ bị hỏng (có thể do gói tin bị cắt ngắn, không thể khôi phục).

Giải pháp là sử dụng TCP cho những loại truyền vận này. TCP cho phép các gói tin có độ dài tùy ý không giới hạn kích thước, và là một giao thức kết nối, có xác nhận, và đáng tin cậy, tự động cung cấp các cơ chế cần thiết để đảm bảo rằng các tác vụ như zone transfer được thực hiện thành công.

2.3. Các cơ chế mở rộng, truyền tải khác

Hiện nay, trong hệ thống DNS, ngoài việc sử dụng các giao thức UDP và TCP cho các truy vấn và phản hồi DNS cơ bản, còn có một số truyền tải mở rộng và cơ chế mới được giới thiệu để cải thiện hiệu suất, bảo mật và khả năng mở rộng của DNS. Dưới đây là một số truyền tải mở rộng quan trọng trong DNS hiện nay:

(1) EDNS0 (Extension Mechanisms for DNS) - Cơ chế mở rộng cho DNS

EDNS0 (được định nghĩa trong RFC 2671) là một cải tiến quan trọng đối với giao thức DNS, cho phép mở rộng khả năng của DNS để hỗ trợ các tính năng hiện tại cũng như các tính năng mới mà không làm thay đổi các giao thức DNS cơ bản. Đặc biệt là hỗ trợ truyền tải các gói tin DNS qua UDP (DNS-over-UDP) có kích thước lớn hơn 512 byte (EDNS0 thường thấy trong các truy vấn/phản hồi truy vấn của DNSSEC, IPv6, ...).

(2) DNS over HTTPS (DoH) - DNS qua HTTPS

DNS over HTTPS (DoH) là một cơ chế mở rộng mới cho phép DNS hoạt động qua giao thức HTTPS thay vì UDP hoặc TCP, giúp ngăn chặn các cuộc tấn công trung gian (Man-in-the-Middle) và che giấu truy vấn DNS khỏi những sự giám sát, thu thập và khai thác dữ liệu, như các cuộc tấn công giám sát mạng hoặc các nhà cung cấp dịch vụ Internet (ISP). Chi tiết về DoH được trình bày trong phần "Mã hóa DNS".

(3) DNS over TLS (DoT) - DNS qua TLS

DNS over TLS (DoT) là một phương pháp mã hóa truy vấn DNS qua giao thức TLS (Transport Layer Security). DoT mã hóa các truy vấn DNS qua TLS, giúp bảo vệ các truy vấn DNS khỏi bị giám sát hoặc tấn công trung gian. DoT sử dụng cổng 853 để truyền tải dữ liệu DNS qua TLS. Chi tiết về DoH được trình bày trong phần "Mã hóa DNS".

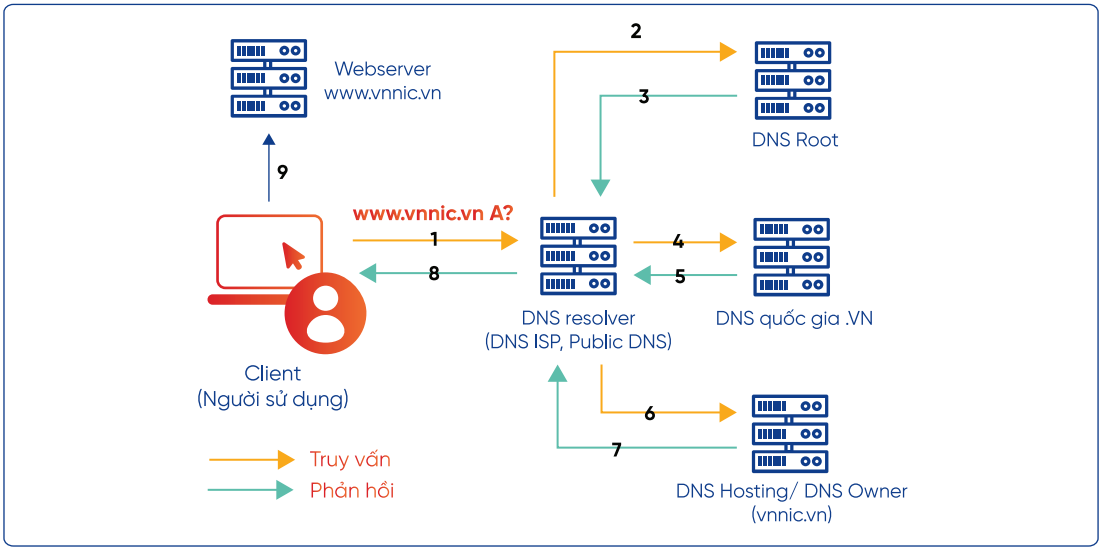
V

MÔ HÌNH HOẠT ĐỘNG CỦA DNS

1. Quá trình phân giải tên miền

Để hiểu rõ về cơ chế truy vấn tên miền chúng ta lấy ví dụ việc truy vấn tên miền www.vnnic.vn. Giả sử người sử dụng muốn truy cập vào trang web có địa chỉ là www.vnnic.vn: Mở trình duyệt web (Cốc Cốc, Microsoft Edge, Google Chrome, Firefox, ...) và gõ tên miền www.vnnic.vn vào thanh địa chỉ của trình duyệt. Quá trình phân giải tên miền diễn ra như sau:

(1) Trước hết chương trình resolver trên máy tính của người sử dụng gửi yêu cầu tìm kiếm địa chỉ IP ứng với tên miền www.vnnic.vn tới máy chủ DNS resolver (thông thường là các máy chủ Recursive DNS của các doanh nghiệp cung cấp dịch vụ Internet-ISP hoặc DNS Public như: DNS Google, DNS Cloudflare, ...). Máy chủ DNS resolver này kiểm tra trong cơ sở dữ liệu (bộ nhớ đệm) của nó có chứa dữ liệu địa chỉ IP của tên miền mà người sử dụng yêu cầu không. Trong trường hợp máy chủ DNS resolver có cơ sở dữ liệu này, nó sẽ gửi kết quả cho người sử dụng.



Hình 14: Các bước truy vấn tên miền www.vnnic.vn

(2) Trong trường hợp máy chủ DNS resolver không có dữ liệu về tên miền, nó sẽ hỏi lên các máy chủ tên miền gốc (DNS Root).

(3) Các máy chủ DNS Root lưu trữ thông tin về các máy chủ tên miền của các tên miền cấp cao (TLD) như .vn, .us, .com, .eu, .org,... Tên miền www.vnnic.vn thuộc về tên miền cấp cao mã quốc gia (ccTLD) ".vn". Máy chủ tên miền DNS Root này sẽ phản hồi cho máy chủ DNS resolver thông tin (địa chỉ IP và tên máy chủ) của các máy chủ tên miền cấp cao mã quốc gia (ccTLD) ".vn" (các máy chủ hệ thống máy chủ DNS quốc gia ".vn").

(4) Máy chủ DNS resolver tiếp tục gửi yêu cầu tìm kiếm địa chỉ IP ứng với tên miền www.vnnic.vn lên các máy chủ của hệ thống máy chủ DNS quốc gia ".vn".

(5) Các máy chủ của hệ thống máy chủ DNS quốc gia ".vn" lưu trữ thông tin chuyển giao của toàn bộ tên miền ".vn", do đó sẽ gửi phản hồi lại máy chủ DNS resolver thông tin các máy chủ DNS chuyển giao (Authoritative DNS Server) của tên miền vnnic.vn (bao gồm địa chỉ IP và tên máy chủ).

(6) Máy chủ DNS resolver sẽ gửi yêu cầu tìm kiếm địa chỉ IP ứng với tên miền www.vnnic.vn lên các máy chủ Authoritative DNS Server quản lý tên miền vnnic.vn.

(7) Do máy chủ quản lý tên miền vnnic.vn có cơ sở dữ liệu về tên miền www.vnnic.vn nên địa chỉ IP của tên miền này sẽ được gửi trả lại cho máy chủ DNS resolver.

(8) Máy chủ DNS resolver chuyển thông tin về địa chỉ IP của tên miền www.vnnic.vn đến máy của người sử dụng.

(9) Người sử dụng dùng địa chỉ IP này để kết nối đến máy chủ chứa trang web có địa chỉ IP do máy chủ DNS resolver trả về.

2. Các loại truy vấn DNS

Hệ thống DNS định nghĩa ba loại truy vấn như sau:

- Truy vấn đệ quy (Recursive queries).
- Truy vấn lặp (Iterative queries)/Truy vấn không đệ quy (Non-recursive queries).
- Truy vấn ngược (Inverse queries).

2.1. Truy vấn đệ quy (Recursive queries)

Truy vấn đệ quy là một loại truy vấn DNS mà máy chủ tên miền (DNS Server) hoặc trình phân giải (resolver) chịu trách nhiệm thực hiện toàn bộ công việc cần thiết để trả lời đầy đủ cho câu hỏi. Việc trả lời một truy vấn đệ quy có thể yêu cầu máy chủ tên miền hoặc trình phân giải gửi nhiều giao dịch truy vấn đến nhiều máy chủ tên miền có thẩm quyền trong hệ thống phân cấp DNS để hoàn tất việc phân giải tên miền được yêu cầu. Các máy chủ tên miền hoặc trình phân giải không bắt buộc phải hỗ trợ truy vấn đệ quy.

- Các phản hồi có thể từ truy vấn đệ quy:
+ Câu trả lời đầy đủ cho truy vấn: Câu trả lời sẽ kèm theo bất kỳ bản ghi CNAME (bí danh) nào có thể hữu ích. Ví dụ, khi truy vấn một bản ghi A (A RR), phản hồi sẽ bao gồm tất cả các bản ghi trong chuỗi CNAME. Phản hồi sẽ chỉ rõ dữ liệu là thẩm quyền (authoritative) hay được lưu trong bộ nhớ tạm (nonauthoritative).
+ Lỗi không tồn tại (NXDOMAIN): Phản hồi báo rằng tên miền hoặc máy chủ không tồn tại. Phản hồi này cũng có thể chứa các bản ghi CNAME trỏ đến máy chủ không tồn tại.
+ Lỗi tạm thời: Ví dụ, khi máy chủ không thể truy cập các máy chủ tên miền khác do lỗi mạng.

- Quy trình truy vấn đệ quy: Trong một truy vấn đệ quy, máy chủ DNS resolver sẽ thay mặt cho trình phân giải (resolver hoặc stub-resolver), truy vấn toàn bộ hệ thống DNS để lấy được câu trả lời chính xác. Dưới đây là quá trình của một truy vấn đệ quy đơn giản, chẳng hạn như truy vấn tên miền www.vnnic.vn:

(1) Người dùng nhập địa chỉ http://www.vnnic.vn vào thanh địa chỉ trên trình duyệt.

(2) Trình duyệt gửi yêu cầu tìm địa chỉ IP của www.vnnic.vn (bản ghi A/AAAA của tên miền www.vnnic.vn) tới trình phân giải cục bộ (stub-resolver).

(3) Stub-resolver gửi truy vấn tới máy chủ DNS resolver (thường là các DNS của các ISP hoặc DNS public như Google DNS, Cloudflare DNS, ...) để yêu cầu tìm địa chỉ IP của www.vnnic.vn.

(4) Máy chủ DNS resolver tra cứu www.vnnic.vn trong bộ nhớ đệm (cache), tuy nhiên trong trường hợp này chỉ xét với những truy vấn DNS lần đầu tiên, do đó sẽ không tìm thấy dữ liệu tên miền trong bộ nhớ đệm.

(5) DNS resolver thực hiện gửi truy vấn tới một trong 13 máy chủ DNS Root với cùng một nội dung truy vấn là yêu cầu tìm địa chỉ IP của www.vnnic.vn.

(6) Máy chủ DNS Root không trả về danh sách các máy chủ Authoritative DNS Server cho cấp tiếp theo trong hệ thống phân cấp tên miền, trong trường hợp này là .vn (được gọi là "referral").

(7) DNS resolver chọn một trong các máy chủ Authoritative DNS Server (ccTLD ".vn") được nhận từ referral và gửi truy vấn để tìm địa chỉ IP của www.vnnic.vn.

(8) Máy chủ ccTLD, trả về danh sách các máy chủ Authoritative DNS Server cho tên miền cấp hai (Second-Level Domain) vnnic.vn (referral).

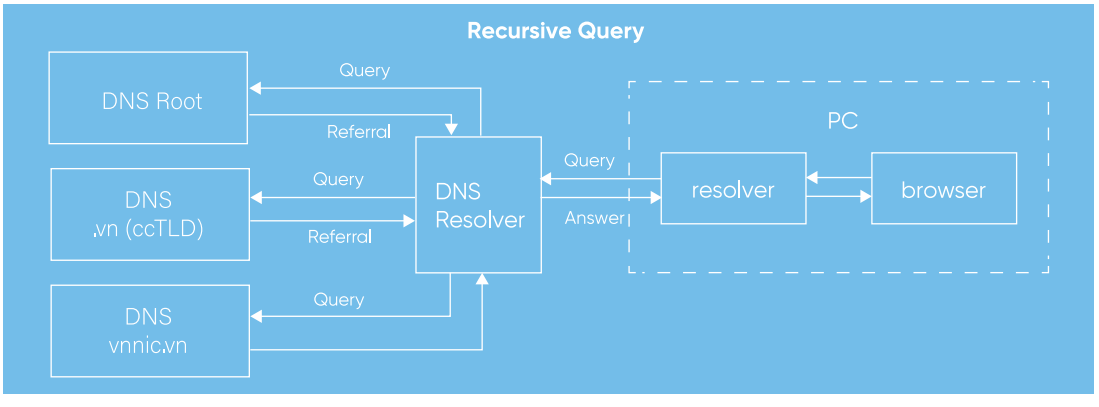
(9) DNS resolver tiếp tục chọn một trong các máy chủ Authoritative DNS Server cho vnnic.vn từ referral trước đó và gửi truy vấn để tìm địa chỉ IP của www.vnnic.vn.

(10) Máy chủ Authoritative DNS Server của vnnic.vn sẽ gửi thông tin bản ghi A/AAAA (địa chỉ IPv4/IPv6) cho DNS resolver.

(11) DNS resolver nhận được câu trả lời và gửi phản hồi địa chỉ IP của www.vnnic.vn tới stub-resolver ban đầu. Đồng thời lưu vào bộ nhớ đệm.

(12) Stub-resolver gửi phản hồi địa chỉ IP của www.vnnic.vn tới trình duyệt của người dùng.

(13) Trình duyệt gửi yêu cầu tới địa chỉ IP để tải trang web.



Hình 15: Truy vấn đệ quy

Trình phân giải stub-resolver trên máy tính của người dùng luôn gửi một truy vấn đệ quy, yêu cầu máy chủ nhận phải thực hiện truy vấn đệ quy và trả về câu trả lời hoàn chỉnh. Khi nhận được truy vấn đệ quy, trình phân giải DNS (DNS Resolver) sẽ bắt đầu quá trình gửi nhiều truy vấn trong hệ thống phân cấp DNS để phân giải hoàn toàn tên miền được yêu cầu.

Trong quá trình này, trình phân giải DNS cũng gửi các truy vấn yêu cầu truy vấn đệ quy tới tất cả các máy chủ Authoritative DNS Server. Tuy nhiên, các máy chủ DNS Root và máy chủ TLD (Top-Level Domain) không bao giờ hỗ trợ đệ quy. Thay vào đó, chúng chỉ trả về thông tin chuyển tiếp (referral) đến cấp tiếp theo trong hệ thống phân cấp.

Khi có nhiều máy chủ tên miền được referral, như trường hợp các máy chủ DNS Root hoặc TLD trong quy trình trên, DNS resolver sẽ lựa chọn máy chủ dựa trên các nguyên tắc sau:

Hầu hết các máy chủ DNS áp dụng một thuật toán để phân bổ tải nhằm đảm bảo kết quả nhanh nhất có thể. Ví dụ đối với phần mềm BIND (Berkeley Internet Name Domain), sẽ sử dụng giá trị RTT (Round Trip Time) để theo dõi thời gian phản hồi từ từng máy chủ DNS đối với các truy vấn. Khi danh sách các máy chủ được cung cấp lần đầu qua một referral, mỗi máy chủ đều có giá trị RTT là 0 (chưa có thông tin về RTT). Trong trường hợp này, BIND sẽ truy cập từng máy chủ một lần theo cơ chế round-robin. Sau khi thu thập được số liệu RTT từ mỗi máy chủ, BIND sẽ ưu tiên sử dụng máy chủ có RTT thấp nhất. BIND tiếp tục sử dụng máy chủ này cho đến khi RTT của nó vượt quá RTT của một máy chủ khác trong danh sách. Lúc này, máy chủ có RTT thấp hơn sẽ trở thành lựa chọn ưu tiên.

Cách tiếp cận này giúp đảm bảo tải được phân phối đều và thời gian phản hồi tối ưu cho người dùng, đồng thời duy trì hiệu quả hoạt động của hệ thống DNS.

2.2. Truy vấn lặp (Iterative queries)

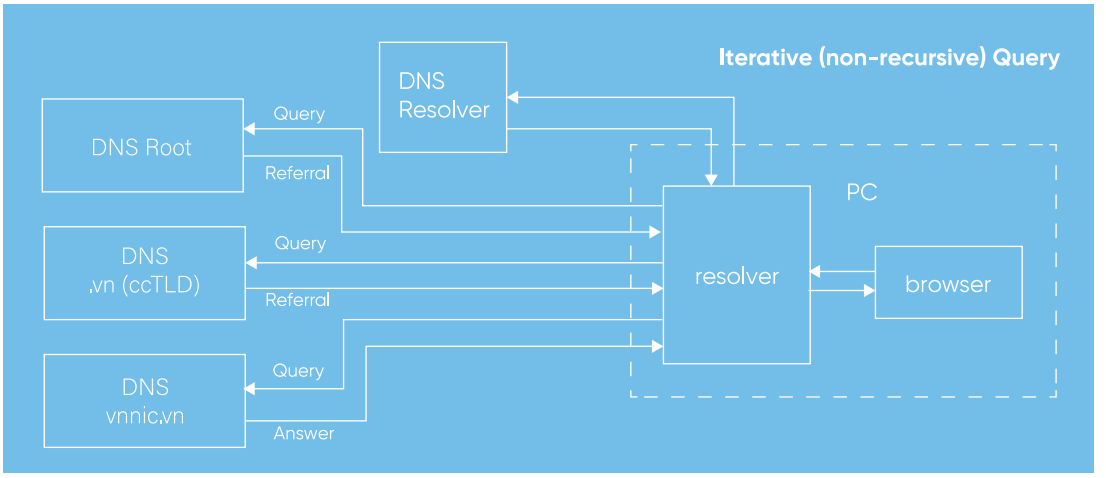
Truy vấn lặp (Iterative queries) hay còn gọi là truy vấn không đệ quy (Non-recursive queries là loại truy vấn mà máy chủ tên miền (DNS server) có thể cung cấp một phần câu trả lời hoặc trả về thông báo lỗi. Các máy chủ tên miền bắt buộc phải hỗ trợ truy vấn không đệ quy.

- Phản hồi có thể từ truy vấn không đệ quy:

+ Câu trả lời đầy đủ cho truy vấn: Phản hồi này bao gồm các bản ghi CNAME (bí danh) đã được sử dụng để xác định tên miền. Phản hồi sẽ chỉ rõ dữ liệu là thẩm quyền (authoritative) hay được lưu trong bộ nhớ tạm (nonauthoritative).
+ Lỗi NXDOMAIN: Phản hồi này thông báo rằng tên miền hoặc máy chủ không tồn tại. Phản hồi này cũng có thể chứa các bản ghi CNAME trỏ đến máy chủ không tồn tại.
+ Lỗi tạm thời: Ví dụ, khi máy chủ không thể truy cập tới các máy chủ DNS khác do lỗi mạng.
+ Thông tin chuyển tiếp (Referral): Phản hồi này chứa danh sách hai hoặc nhiều máy chủ tên miền và địa chỉ IP của chúng, thường là các máy chủ ở cấp kế tiếp trong hệ thống phân cấp tên miền. Các máy chủ này có thể, hoặc không phải là máy chủ Authoritative DNS Server cuối cùng cho tên miền được truy vấn.

Phản hồi dạng referral là phương pháp trả lời tiêu chuẩn của máy chủ DNS Root và máy chủ TLD (Top-Level Domain), vì các loại máy chủ này chỉ hỗ trợ truy vấn không đệ quy.

- Quy trình hoạt động của truy không đệ quy: Quy trình của một truy vấn không đệ quy đơn giản như gửi một truy vấn, yêu cầu phân giải tên miền www.vnnic.vn tới một máy chủ tên miền chỉ hỗ trợ truy vấn không đệ quy nhưng không phải máy chủ Authoritative DNS Server cho tên miền vnnic.vn diễn ra tương tự với quy trình truy vấn đệ quy, tuy nhiên trong trường hợp này DNS resolver sẽ không đóng vai trò là một máy chủ truy vấn không đệ quy, do đó, khi resolver gửi truy vấn yêu cầu tìm kiếm địa chỉ IP của www.vnnic.vn thì DNS resolver sẽ gửi lại resolver một danh sách các máy chủ DNS Root, để resolver thực hiện các truy vấn tiếp theo cho đến khi resolver nhận được phản hồi cuối cùng.



Hình 16: Truy vấn lặp/không đệ quy

2.3. Truy vấn ngược (Inverse Queries)

Truy vấn ngược (Inverse Query) là quá trình ánh xạ từ một bản ghi tài nguyên (RR) đến một tên miền. Ví dụ về truy vấn ngược có thể là: "Tên miền nào được gắn với bản ghi MX này?".

Trong các tiêu chuẩn DNS, việc hỗ trợ truy vấn ngược luôn được định nghĩa là một tùy chọn. Trong trường hợp này, các máy chủ tên miền có thể trả về phản hồi "Không được triển khai" (NOTIMP). Do đó, truy vấn ngược không được sử dụng rộng rãi và dần bị loại bỏ hoàn toàn khi được tuyên bố là lỗi thời trong tiêu chuẩn RFC 3425.

Quá trình ánh xạ từ địa chỉ IP đến tên miền được gọi là phân giải ngược (reverse mapping) hoặc tra cứu ngược (reverse lookup). Quá trình này sử dụng các truy vấn đệ quy hoặc lặp thông thường với một tên miền đặc biệt: IN-ADDR.ARPA.

Phân giải ngược DNS (DNS Reverse Mapping):

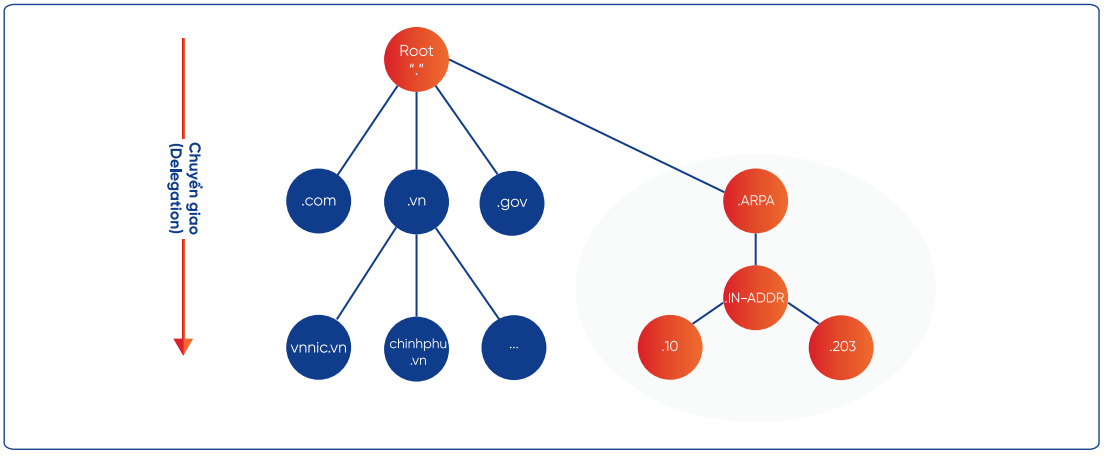
Thông thường, một truy vấn DNS sẽ phân giải và xác định địa chỉ IP của một tên miền. Tuy nhiên, trong một số trường hợp, cần xác định tên của máy chủ dựa trên địa chỉ IP cụ thể. Quá trình này được gọi là phân giải ngược (reverse mapping).

Phân giải ngược thường được sử dụng vì lý do bảo mật, chẳng hạn như truy tìm nguồn gốc của hacker hoặc spammer. Hầu hết các hệ thống gửi email hiện đại sử dụng phân giải ngược để cung cấp một phương thức xác thực đơn giản, kiểm tra rằng địa chỉ IP đã cho tương ứng với tên máy chủ được chỉ định thông qua chính sách truy vấn DNS (DNS lookup policies).

Để thực hiện phân giải ngược, hệ thống DNS định nghĩa một miền đặc biệt (reserved domain) có tên IN-ADDR.ARPA. Miền này được sử dụng để thực hiện các truy vấn đệ quy và lặp thông thường nhằm ánh xạ địa chỉ IP thành tên miền.

Lưu ý:

Miền IN-ADDR.ARPA có thể được viết dưới dạng chữ thường (in-addr.arpa), vì DNS không phân biệt chữ hoa và chữ thường. Tuy nhiên, theo tiêu chuẩn, cách viết hoa được duy trì giữa các truy vấn và phản hồi, do đó, cách viết IN-ADDR.ARPA thường được sử dụng.



Hình 17: Chuyển giao tên miền ngược

Như trình bày ở trên, phân giải ngược sử dụng miền đặc biệt IN-ADDR.ARPA, với cách đảo ngược thứ tự địa chỉ IP để phù hợp với cấu trúc phân cấp DNS. Cách tiếp cận này duy trì sự thống nhất với hệ thống DNS, đồng thời đảm bảo tính hiệu quả trong các truy vấn ngược để xác định tên máy chủ từ địa chỉ IP.

Ví dụ về tệp dữ liệu zone tên miền phân giải ngược dành cho tên miền vnnic.vn:

```
; Tệp dữ liệu zone tên miền phân giải ngược đơn giản cho vn-
nic.vn
$TTL 2d ; TTL mặc định cho zone
$ORIGIN 254.168.192.IN-ADDR.ARPA.

@ IN SOA ns1.vnnic.vn. hostmaster.vnnic.vn. (
  2003080800 ; sn = serial number
  12h        ; refresh
  15m        ; retry
  3w         ; expiry
  2h         ; nxdomain ttl
)

   IN NS ns1.vnnic.vn.
   IN NS ns2.vnnic.net.vn.

; Bản ghi PTR ánh xạ địa chỉ IPv4 tới tên máy chủ
2  IN PTR ns1.vnnic.vn.
4  IN PTR mail.vnnic.vn.
16 IN PTR joe.vnnic.vn.
```

Lưu ý:

- Các bản ghi PTR sử dụng tên miền đầy đủ (FQDN - Fully Qualified Domain Names) kết thúc bằng một dấu chấm (.) do quy tắc thay thế $ORIGIN. Quy tắc này tự động bổ sung gốc của zone ($ORIGIN) vào bất kỳ tên miền nào không kết thúc bằng dấu chấm.

- Tệp dữ liệu zone tên miền phân giải ngược giúp đảm bảo quá trình ánh xạ địa chỉ IP thành tên miền diễn ra chính xác, đóng vai trò quan trọng trong xác thực và các dịch vụ liên quan đến DNS.

3. Mô hình Client-Server trong DNS

Hệ thống máy chủ tên miền được thiết kế hoạt động dựa trên mô hình Client-Server, là mô hình cơ bản và phổ biến, đóng vai trò nền tảng cho hoạt động của Internet. Mô hình này cung cấp cách thức tổ chức và vận hành phân cấp, đảm bảo hiệu suất cao, tính mở rộng và khả năng chịu lỗi. Đây là cơ chế giúp hàng tỷ yêu cầu phân giải tên miền mỗi ngày được xử lý một cách chính xác, ổn định và nhanh chóng.

3.1. Cấu trúc và nguyên lý hoạt động

Trong mô hình Client-Server của máy chủ tên miền, mỗi thành phần đảm nhận một vai trò cụ thể, tạo nên sự phối hợp nhịp nhàng để thực hiện quá trình phân giải tên miền thành địa chỉ IP và ngược lại. Hai thành phần chính của mô hình này là Resolver (Client) và DNS Server (Server).

(1) Resolver (Client): Resolver là thành phần nằm ở phía người dùng, chịu trách nhiệm khởi tạo các yêu cầu phân giải tên miền. Khi một người dùng nhập một tên miền vào trình duyệt web, Resolver sẽ gửi một truy vấn DNS (DNS query) để tìm địa chỉ IP tương ứng.

Resolver thường được tích hợp vào hệ điều hành hoặc các ứng dụng trên thiết bị của người dùng, như trình duyệt hoặc máy chủ ứng dụng. Nó cũng có khả năng lưu trữ tạm thời (caching) các kết quả phân giải trước đó để giảm thiểu độ trễ và giảm tải cho hệ thống DNS.

(2) DNS Server (Server): DNS Server là thành phần chịu trách nhiệm xử lý các truy vấn từ Resolver và cung cấp thông tin chính xác về địa chỉ IP của tên miền. DNS Server hoạt động ở nhiều cấp độ trong cấu trúc phân cấp của DNS, bao gồm:

- DNS Root: Điểm khởi đầu của hệ thống DNS toàn cầu, cung cấp thông tin về các máy chủ quản lý tên miền cấp cao nhất - Top-Level Domain (TLD DNS Server).
- TLD DNS Server: Quản lý các tên miền cấp cao nhất (như .vn, .us, .com, .net, ...) và cung cấp thông tin về các máy chủ DNS có thẩm quyền (Authoritative DNS Server).
- Authoritative DNS Server: Cung cấp thông tin chính thức về tên miền, bao gồm các bản ghi DNS (như A, AAAA, MX, TXT, ...) của các tên miền mà nó chịu trách nhiệm quản lý.

3.2. Quy trình phân giải tên miền

Quy trình hoạt động của mô hình Client-Server trong hệ thống DNS được thực hiện theo các bước sau:

- Khởi tạo truy vấn từ Resolver: Khi người dùng nhập một URL (ví dụ: www.vnnic.vn) vào trình duyệt, Resolver sẽ gửi một truy vấn để tìm địa chỉ IP của tên miền này.
- Truy vấn DNS Root: Nếu kết quả không có sẵn trong bộ nhớ đệm, Resolver sẽ gửi truy vấn đến DNS Root để nhận thông tin về TLD DNS Server liên quan đến tên miền (như ccTLD ".vn").
- Truy vấn TLD DNS Server: DNS Root trả về địa chỉ IP của TLD DNS Server, và Resolver tiếp tục gửi truy vấn đến TLD DNS Server để tìm thông tin về Authoritative DNS Server của tên miền vnnic.vn.
- Truy vấn Authoritative DNS Server: TLD DNS Server trả về địa chỉ IP của Authoritative DNS Server, nơi lưu trữ thông tin chính thức của tên miền. Resolver gửi truy vấn đến Authoritative DNS Server để nhận địa chỉ IP của www.vnnic.vn.
- Trả về kết quả: Authoritative DNS Server trả về địa chỉ IP của tên miền. Resolver lưu kết quả này vào bộ nhớ đệm và cung cấp thông tin cho trình duyệt, giúp trình duyệt kết nối đến máy chủ web.

3.3. Lợi ích của mô hình Client-Server trong DNS

Mô hình Client-Server trong hệ thống DNS mang lại nhiều lợi ích nổi bật, bao gồm:

- Cấu trúc phân cấp và phân tán: Hệ thống DNS được tổ chức theo mô hình phân cấp với nhiều cấp máy chủ (Root, TLD, Authoritative), giúp phân phối tải truy vấn và đảm bảo hệ thống có thể mở rộng để đáp ứng nhu cầu truy cập toàn cầu. Cấu trúc phân tán này cũng làm giảm nguy cơ tắc nghẽn và tăng độ sẵn sàng của dịch vụ.
- Tăng hiệu suất truy vấn: Các máy khách (client) sử dụng bộ phân giải (resolver) có cơ chế lưu trữ tạm thời (cache), giúp giảm thiểu số lần truy vấn đến máy chủ DNS và tăng tốc độ phản hồi cho người dùng.
- Đảm bảo tính ổn định và tin cậy: Dữ liệu DNS được phân phối trên nhiều máy chủ khác nhau. Nhờ đó, khi một máy chủ gặp sự cố, hệ thống vẫn có thể hoạt động bình thường nhờ các máy chủ thay thế. Điều này giúp duy trì tính liên tục của dịch vụ và giảm thời gian gián đoạn.

3.4. Hạn chế và giải pháp

Mặc dù hiệu quả, nhưng mô hình Client-Server trong DNS không tránh khỏi một số thách thức:

- Tính phụ thuộc vào máy chủ trung tâm (single point of failure): Trong mô hình Client-Server, client phụ thuộc hoàn toàn vào các máy chủ DNS để phân giải tên miền. Nếu một máy chủ quan trọng không khả dụng mà không có phương án dự phòng, việc phân giải tên miền sẽ thất bại, gây gián đoạn dịch vụ.
- Khó khăn trong mở rộng theo chiều ngang: Mô hình Client-Server không mở rộng tự nhiên như mô hình phân tán ngang (peer-to-peer).
- Tốn thời gian thiết lập kết nối và phản hồi: Trong mô hình Client-Server, mỗi truy vấn cần thiết lập kết nối tới một máy chủ cụ thể (qua UDP/TCP). Khi hệ thống phân cấp DNS có nhiều lớp máy chủ (Root, TLD, Authoritative), điều này làm gia tăng số lần tương tác client-server.

Các vấn đề hạn chế này được giải quyết bằng việc ứng dụng, kết hợp nhiều giải pháp, công nghệ khác nhau như: Triển khai máy chủ, hệ thống dự phòng, tính sẵn sàng cao (High Availability - HA); ứng dụng Anycast nhằm phân tán, đưa máy chủ, dịch vụ DNS đến gần người dùng nhất; sử dụng các hệ thống Recursive DNS trung gian để lưu trữ đệm các kết quả phân giải tên miền;...

VI

KIẾN TRÚC DNS

Hệ thống máy chủ tên miền (DNS Server) là một trong những hạ tầng quan trọng nhất của Internet, được thiết kế với tính linh hoạt và khả năng mở rộng cao. Kiến trúc của DNS dựa trên nguyên tắc phân tán, giúp quản lý khối lượng dữ liệu khổng lồ và đảm bảo hiệu quả hoạt động. Bên cạnh đó, hệ thống DNS còn có kiến trúc Master-Slave, đây là cơ chế đóng vai trò quan trọng trong việc duy trì tính nhất quán và dự phòng trong quản lý dữ liệu DNS.

1. Kiến trúc phân tán

Kiến trúc phân tán là nền tảng cốt lõi của hệ thống máy chủ DNS, trong đó toàn bộ dữ liệu được chia nhỏ và phân phối trên nhiều máy chủ khắp toàn cầu. Hệ thống máy chủ DNS không phụ thuộc vào một máy chủ trung tâm, mà thay vào đó, sử dụng một mạng lưới các máy chủ DNS được tổ chức theo mô hình phân cấp (hierarchical), gồm các máy chủ như đã trình bày tại mục II.3 (2) – Phần 1 ở trên. Kiến trúc phân tán này mang lại nhiều lợi ích:

- Khả năng mở rộng: Cho phép quản lý hàng tỷ tên miền mà không gây áp lực lên một hệ thống trung tâm.
- Tính sẵn sàng: Hệ thống vẫn tiếp tục hoạt động ngay cả khi một hoặc nhiều máy chủ DNS gặp sự cố.
- Hiệu quả: Các máy chủ DNS cục bộ (Local DNS[7]) sử dụng bộ nhớ đệm (cache) để lưu trữ tạm thời các kết quả truy vấn, giúp giảm tải cho các máy chủ cấp cao hơn và tăng tốc độ phản hồi.

Kiến trúc phân tán không chỉ đảm bảo hiệu suất mà còn đóng vai trò quan trọng trong bảo mật, giảm thiểu rủi ro tấn công vào một điểm duy nhất (single point of failure).

2. Mô hình Master-Slave

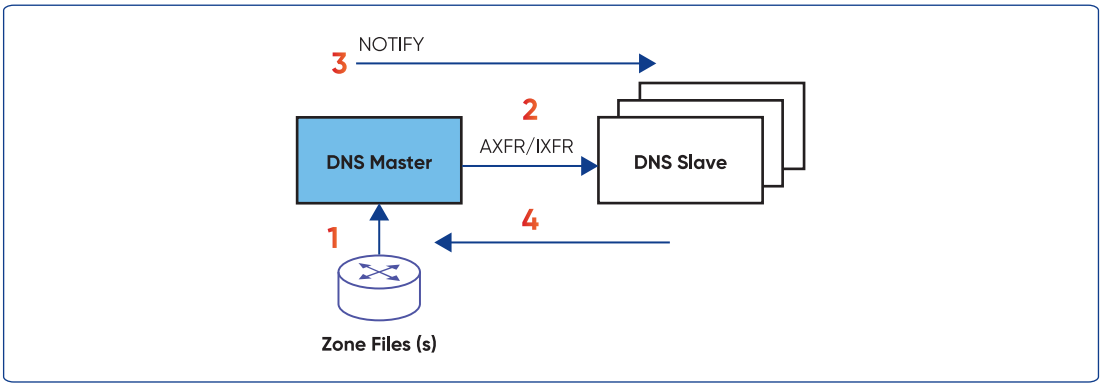
Mô hình Master-Slave là một cơ chế quan trọng trong quản lý và duy trì dữ liệu DNS, trong đó:

- **Master Server (Máy chủ chính):** Là nơi dữ liệu gốc của một zone tên miền được quản lý và cập nhật. Các thay đổi như thêm, sửa, hoặc xóa các bản ghi DNS được thực hiện trên máy chủ chính.
- **Slave Server (Máy chủ phụ):** Là bản sao của máy chủ chính, lưu trữ dữ liệu DNS nhận được từ máy chủ chính thông qua cơ chế đồng bộ (zone transfer). Máy chủ phụ hoạt động như một máy chủ dự phòng để đảm bảo tính khả dụng của dữ liệu ngay cả khi máy chủ chính không hoạt động.

Mô hình Master-Slave được ứng dụng trong triển khai các máy chủ DNS Root, TLD DNS Server và Authoritative DNS Server.

- **Ưu điểm của mô hình Master-Slave:**
  - Đảm bảo tính sẵn sàng: Trong trường hợp máy chủ chính gặp sự cố, máy chủ phụ vẫn có thể phục vụ các truy vấn DNS.
  - Cân bằng tải: Các truy vấn DNS được phân phối giữa máy chủ chính và máy chủ phụ, giảm áp lực lên một máy chủ duy nhất.
  - Tính nhất quán: Các bản sao dữ liệu DNS trên máy chủ phụ được đồng bộ hóa định kỳ từ máy chủ chính thông qua cơ chế zone transfer, đảm bảo tính chính xác của dữ liệu trên toàn hệ thống.
- **Hoạt động của mô hình Master-Slave:**
  - Cập nhật dữ liệu trên máy chủ chính: Các bản ghi DNS được thay đổi hoặc cập nhật tại máy chủ chính.
  - Truyền dữ liệu đến máy chủ phụ: Thông qua cơ chế đồng bộ (AXFR – đồng bộ toàn phần hoặc IXFR – đồng bộ một những thay đổi), dữ liệu được sao chép từ máy chủ chính đến máy chủ phụ.
  - Trả lời truy vấn: Cả máy chủ chính và máy chủ phụ đều có khả năng trả lời các truy vấn DNS, tùy thuộc vào cấu hình của hệ thống.

[7] Local DNS: là một máy chủ DNS nằm trong mạng nội bộ hoặc gần với người dùng, thường được sử dụng để xử lý các yêu cầu DNS từ các thiết bị trong cùng một mạng.



Hình 18: Mô hình Master-Slave

Mô hình Master-Slave đóng vai trò quan trọng trong việc đảm bảo tính ổn định, nhất quán, và bảo mật của hệ thống DNS. Đặc biệt, trong các môi trường doanh nghiệp lớn hoặc các tổ chức cần quản lý nhiều tên miền, mô hình này giúp giảm thiểu rủi ro và tối ưu hóa hiệu suất hoạt động.

3. Các loại máy chủ DNS

Mỗi loại máy chủ DNS (DNS Server) đều có vai trò riêng, đảm bảo việc quản lý và phân giải tên miền trong hệ thống DNS. Sau đây là phân loại các loại máy chủ DNS:

3.1. Máy chủ chính: Primary/Master DNS Server

Máy chủ chính, hay còn gọi là Primary DNS Server hoặc Master DNS Server, hoặc có thể gọi ngắn gọn là DNS Primary, DNS Master. Máy chủ chính chịu trách nhiệm quản lý và lưu trữ dữ liệu chính thức của một zone tên miền. Đây là nơi tất cả các bản ghi tài nguyên (Resource Records) được tạo mới, chỉnh sửa hoặc xóa, và được coi là nguồn dữ liệu chính thức cho zone mà nó quản lý.

- **Đặc điểm và vai trò:**

+ Quản lý dữ liệu gốc: Primary DNS Server lưu trữ các tệp dữ liệu zone tên miền (zone file) chứa thông tin chi tiết về các bản ghi DNS như bản ghi A, MX, NS, CNAME, ...
+ Cung cấp thông tin: Primary DNS Server trả lời các truy vấn từ các máy chủ khác hoặc từ các ứng dụng yêu cầu thông tin về tên miền mà nó có thẩm quyền.
+ Đồng bộ (zone transfer): Primary DNS Server đồng bộ dữ liệu tới các máy chủ phụ (Secondary DNS Server) thông qua cơ chế đồng bộ zone transfer, đảm bảo tính nhất quán của dữ liệu.
  Primary DNS Server đóng vai trò trung tâm trong hệ thống DNS. Nếu xảy ra sự cố hoặc lỗi cấu hình trên máy chủ này, dữ liệu gốc có thể bị sai lệch, ảnh hưởng đến toàn bộ hệ thống phân giải tên miền.

3.2. Máy chủ phụ: Secondary/Slave DNS Server

Máy chủ phụ hay còn gọi là Secondary DNS Server hoặc Slave DNS Server, hoặc có thể gọi ngắn gọn là DNS Secondary, DNS Slave. Máy chủ phụ là bản sao của Primary DNS Server, được thiết kế để hoạt động như một hệ thống dự phòng và hỗ trợ. Dữ liệu của Secondary DNS Server được sao chép từ Primary DNS Server thông qua cơ chế đồng bộ (zone transfer), đảm bảo rằng cả hai máy chủ lưu trữ cùng một bộ dữ liệu.

- **Đặc điểm và vai trò:**

+ Dự phòng: Secondary DNS Server hoạt động như một bản sao dự phòng của Primary DNS Server, giúp đảm bảo hệ thống vẫn hoạt động bình thường ngay cả khi Primary DNS Server gặp sự cố.
+ Phân tải: Các truy vấn DNS có thể được phân phối giữa Primary và Secondary để giảm áp lực lên một máy chủ duy nhất.
+ Tăng cường khả dụng: Secondary DNS Server giúp tăng khả năng truy cập dữ liệu từ nhiều địa điểm khác nhau, cải thiện hiệu suất và độ tin cậy của hệ thống DNS.

- **Hoạt động:**

+ Đồng bộ (zone transfer): Secondary DNS Server định kỳ nhận dữ liệu từ Primary DNS Server thông qua các cơ chế như AXFR (Full Zone Transfer) hoặc IXFR (Incremental Zone Transfer).
+ Trả lời truy vấn: Secondary DNS Server có thể trả lời các truy vấn DNS như Primary DNS Server, giúp giảm tải và tăng tốc độ phản hồi cho người dùng.
  Máy chủ chính và máy chủ phụ là một loại máy chủ Authoritative DNS Server trong mô hình phân cấp hệ thống DNS.

3.3. Máy chủ đệm: DNS Caching

DNS Caching là một loại máy chủ không lưu trữ dữ liệu gốc mà thay vào đó, lưu trữ tạm thời các kết quả truy vấn DNS trước đó trong bộ nhớ đệm (cache). Loại máy chủ này chủ yếu phục vụ việc tăng tốc độ phân giải tên miền và giảm tải cho các máy chủ DNS khác trong hệ thống.

- **Đặc điểm và vai trò:**

+ Tăng tốc truy vấn: Khi nhận được một truy vấn, DNS Caching sẽ kiểm tra bộ nhớ đệm trước. Nếu dữ liệu đã được lưu trữ trong bộ nhớ đệm, nó sẽ trả lời truy vấn ngay lập tức mà không cần liên lạc với các máy chủ DNS khác.
+ Giảm tải hệ thống: Bằng cách lưu trữ tạm thời các kết quả truy vấn, DNS Caching giảm số lượng truy vấn cần phải gửi đến DNS Root, TLD DNS Server và Authoritative DNS Server.
+ Tối ưu hóa hiệu suất: Với dữ liệu được lưu trữ trong bộ nhớ đệm, DNS Caching cải thiện đáng kể thời gian phản hồi cho người dùng cuối.

- **Cơ chế hoạt động:**

+ Lưu trữ tạm thời: Kết quả truy vấn DNS được lưu trữ trong khoảng thời gian xác định bởi giá trị TTL (Time-To-Live) của từng bản ghi.
+ Làm mới dữ liệu: Khi giá trị TTL của một bản ghi hết hạn, DNS Caching sẽ gửi truy vấn mới đến các máy chủ DNS khác để cập nhật dữ liệu.

3.4. Máy chủ chuyển tiếp: Forwarding (Proxy) DNS Server

Máy chủ chuyển tiếp, hay còn gọi là máy chủ proxy, là loại máy chủ DNS nhận yêu cầu từ các máy khách và chuyển tiếp chúng đến máy chủ DNS khác để lấy thông tin. Chức năng chính của máy chủ này là giảm tải cho các máy chủ DNS chính và cải thiện hiệu suất bằng cách lưu trữ các kết quả truy vấn trong bộ nhớ đệm.

3.5. Máy chủ ẩn: Stealth (DMZ or Split) DNS Server

Máy chủ ẩn là máy chủ DNS được cấu hình để không công bố thông tin của ra ngoài. Máy chủ này thường được sử dụng trong các môi trường bảo mật, như DMZ (Demilitarized Zone), để bảo vệ thông tin của các máy chủ nội bộ. Máy chủ này có thể cung cấp thông tin khác nhau cho các đối tượng khác nhau, tùy thuộc vào vị trí của yêu cầu.

VII

PHÂN LOẠI BẢN GHI DNS

1. Các bản ghi chính

1.1. Bản ghi SOA

Bản ghi được khai báo đầu tiên trong file dữ liệu là bản ghi SOA (Start Of Authority). Bản ghi SOA chỉ ra máy chủ tên miền này chính là nơi lưu giữ dữ liệu cho tất cả các tên miền thuộc tên miền được khai báo trong file này. Mỗi file dữ liệu chỉ có một bản ghi SOA duy nhất.

Cấu trúc của bản ghi SOA như sau:

```
<Tên miền> <class> SOA <tên máy chủ> <địa chỉ e-mail> (
                                Serial number
                                Refresh time
                                Retry time
                                Expire time
                                Time to live
                                );
```

Ví dụ:

```
vnnic.vn.          IN SOA dns1.vnnic.vn. postmaster.vnnic.vn. (
                      2023034257 ; serial
                      1800       ; refresh (30 minutes)
                      900        ; retry (15 minutes)
                      604800     ; expire (1 week)
                      5400       ; minimum (1 hour 30 minutes)
                      )
```

Theo cấu trúc như trên, thông tin đầu tiên được khai báo trong bản ghi SOA là tên miền (vnnic.vn) được khai báo trong file dữ liệu.

Trường IN: Trường IN chỉ ra rằng tên miền này được sử dụng trong mạng Internet.

Tiếp sau trường SOA là tên của máy chủ tên miền và địa chỉ e-mail của người quản trị tên miền này.

Trong ví dụ trên, tên miền vnnic.vn được khai báo trên máy chủ dns1.vnnic.vn và địa chỉ e-mail của người quản lý tên miền vnnic.vn là postmaster@vnnic.vn.

Các thông số tiếp theo được khai báo trong bản ghi SOA là:

- **Serial number:** Đây là giá trị được áp dụng cho tất cả dữ liệu trong một zone. Khi máy chủ thứ cấp kết nối với máy chủ chính để thực hiện chuyển các file dữ liệu về, máy chủ thứ cấp sẽ hỏi máy chủ chính giá trị serial number của zone mà nó muốn lấy dữ liệu. Nếu như giá trị Serial number ở máy thứ cấp nhỏ hơn giá trị serial number ở máy chủ chính thì máy chủ thứ cấp sẽ thực hiện lấy dữ liệu từ máy chủ chính. Vì vậy khi có bất cứ sự thay đổi nào về dữ liệu tại máy chủ chính, người quản trị DNS phải thực hiện tăng giá trị serial number lên để máy chủ thứ cấp thực hiện chuyển file dữ liệu. Giá trị Serial number là một số nguyên có thể thay đổi từ 0 đến 4294967295.
- **Expire time:** Đây là khoảng thời gian mà nếu máy chủ tên miền thứ cấp không thể kết nối với máy chủ tên miền chính, dữ liệu trên máy chủ thứ cấp sẽ bị huỷ không được dùng. Theo khai báo ở ví dụ trên nếu sau 604.800 giây mà máy chủ thứ cấp không thể kết nối với máy chủ chính thì dữ liệu trên máy chủ thứ cấp sẽ bị huỷ.
- **Time to live (TTL):** Đây là giá trị áp dụng cho tất cả các bản ghi trong file dữ liệu, tham số thời gian này xác định dữ liệu sẽ được lưu trữ tại máy chủ tên miền trong bao lâu. Lưu ý: có 02 kiểu TTL là positive TTL và negative TTL.

- **Positive TTL:** Là giá trị TTL cho biết thời gian (tính bằng giây) mà bản ghi sẽ được lưu trữ. Ví dụ: Nếu TTL là 3600 giây (1 giờ), bản ghi sẽ được sử dụng trong 1 giờ trước khi máy chủ DNS phải kiểm tra lại để xem có bản ghi mới không. Positive TTL giúp giảm tải cho máy chủ DNS và cải thiện tốc độ truy cập bằng cách giảm số lần cần phải truy vấn lại.
- **Negative TTL:** Là giá trị TTL xác định thời gian mà các máy chủ DNS sẽ lưu trữ thông tin về việc không tìm thấy tên miền hoặc không thể truy vấn được bản ghi cho một tên miền (tức là khi tên miền đó không tồn tại hoặc bị lỗi) trong bộ nhớ đệm (cache). Giúp các máy chủ DNS nhận biết rằng bản ghi không tồn tại và không thử truy vấn lại trong một khoảng thời gian nhất định. Negative TTL giúp giảm thiểu số lượng truy vấn thất bại đến máy chủ DNS, từ đó cải thiện hiệu suất tổng thể của hệ thống.

1.2. Bản ghi NS

Bản ghi NS (DNS Server Resource Record) là một thành phần quan trọng trong hệ thống DNS (Domain Name System), được tiêu chuẩn hóa trong RFC 1035. Chức năng chính của bản ghi NS là chỉ định các máy chủ tên miền có thẩm quyền quản lý và chịu trách nhiệm cung cấp thông tin cho một zone hoặc tên miền cụ thể. Đây là bản ghi nền tảng, giúp định hướng các truy vấn DNS đến đúng máy chủ cần thiết, đảm bảo hệ thống DNS hoạt động chính xác và hiệu quả.

Mỗi zone tên miền DNS phải có ít nhất hai bản ghi NS để đảm bảo tính dự phòng và độ tin cậy. Các máy chủ tên miền được khai báo trong bản ghi NS phải có khả năng trả lời các truy vấn DNS liên quan đến zone mà chúng quản lý.

Cú pháp cơ bản của một bản ghi NS được mô tả như sau:

```
<Tên miền> <TTL> <Lớp> <Loại bản ghi> <Tên máy chủ DNS>
```

Trong đó:

Tên miền (name): Chỉ định tên miền hoặc zone tên miền mà bản ghi NS áp dụng.

TTL (Time to Live): Thời gian lưu trữ bản ghi trong bộ nhớ đệm.

Lớp (class): Lớp mạng, thông thường là "IN" (Internet).

Loại bản ghi (rr): Loại bản ghi, ở đây là "NS".

Tên máy chủ DNS (name-server): Tên của máy chủ Authoritative DNS Server, được khai báo dưới dạng FQDN (Fully Qualified Domain Name).

1.3. Bản ghi A

Bản ghi A (Address Record) là một trong những bản ghi DNS cơ bản và phổ biến nhất, dùng để ánh xạ tên miền (domain name) tới địa chỉ IPv4. Nó cho phép trình phân giải DNS (resolver) phân giải tên miền mà con người dễ nhớ thành địa chỉ IP, từ đó thiết lập kết nối mạng giữa máy khách (client) và máy chủ (server). Đây là nền tảng quan trọng cho các dịch vụ trực tuyến hoạt động trên giao thức IPv4.

Bản ghi A được tiêu chuẩn hóa trong RFC 1035 và định nghĩa địa chỉ IPv4 của một máy chủ cụ thể trong miền hoặc zone. Bản ghi tương đương cho IPv6 là bản ghi AAAA.

Cú pháp chính thức của bản ghi A như sau:

```
name ttl class rr ipv4
```

Ví dụ, các bản ghi A được định nghĩa như sau:

```
ns1   IN  A   192.168.254.2
mail  IN  A   192.168.254.4
joe   IN  A   192.168.254.6
www   IN  A   192.168.254.7
```

CÚ PHÁP	VÍ DỤ SỬ DỤNG	MÔ TẢ
name	ns1	Tên miền dạng rút gọn, sử dụng sự thay thế $ORIGIN. Chúng ta có thể viết điều này dưới dạng ns1.vnnic.vn (dùng FQDN - Fully Qualified Domain Name) để dễ hiểu hơn.
ttl		Không có TTL nào được định nghĩa cho bản ghi RR, vì vậy giá trị mặc định của zone (2 ngày, được định nghĩa trong lệnh $TTL) sẽ được sử dụng.
class	IN	Xác định class là Internet.
IPv4	192.168.254.2	Định nghĩa rằng host ns1 có địa chỉ IPv4 là 192.168.254.2. Các bản ghi được định nghĩa bởi NS hoặc MX RR phải có các bản ghi A tương ứng trong zone để phân giải các tên miền con như ns1 và mail. Bất kỳ host nào mà người dùng muốn công khai cũng cần được định nghĩa bằng bản ghi A; trong ví dụ này, các bản ghi bao gồm dịch vụ web (www) và tên host joe

Chúng ta có thể gán, khai báo địa chỉ IP giống nhau với nhiều tên miền khác nhau như được minh họa trong ví dụ sau (ở đây, máy chủ tên miền và máy chủ web được đặt cùng trên một máy):

```
ns1   IN  A   192.168.254.2
mail  IN  A   192.168.254.4
joe   IN  A   192.168.254.6
www   IN  A   192.168.254.2
```

Hoặc, cũng có thể sử dụng bản ghi CNAME (sẽ được mô tả trong phần tiếp theo). Nhiều địa chỉ IP cũng có thể được định nghĩa cho cùng một host như trong ví dụ dưới đây, có 03 địa chỉ IPv4 được cung cấp cho host www.vnnic.vn.

```
www   IN  A   192.168.254.2
      IN  A   192.168.254.7
      IN  A   192.168.254.8
```

Phần mềm DNS thường sẽ cung cấp các địa chỉ IP được định nghĩa theo thứ tự vòng lặp ngẫu nhiên (round-robin) hoặc được chỉ định, tùy thuộc vào cấu hình của người quản trị. Tính năng này có thể được sử dụng để cung cấp khả năng cân bằng tải hoặc tăng khả năng phục hồi của các dịch vụ.

Trong ví dụ trên, khi một máy khách yêu cầu bản ghi A liên quan đến www.vnnic.vn, máy chủ DNS có thể phản hồi với một địa chỉ ngẫu nhiên hoặc một địa chỉ theo thứ tự.

1.4. Bản ghi AAAA

Bản ghi AAAA (Quad-A Record) là một loại bản ghi DNS được sử dụng để ánh xạ tên miền tới địa chỉ IPv6. Bản ghi này được định nghĩa trong RFC 3596 và mở rộng từ bản ghi A vốn dành cho địa chỉ IPv4. Với sự phát triển của IPv6 nhằm giải quyết vấn đề cạn kiệt địa chỉ IPv4, AAAA đóng vai trò quan trọng trong việc hỗ trợ hoạt động của các dịch vụ trên môi trường mạng hiện đại.

Cú pháp cơ bản của bản ghi AAAA như sau:

```
name   ttl   class   rr   ipv6-address
```

Ví dụ:

```
www    IN    AAAA    2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Trong ví dụ này:

- www là tên miền.
- IN chỉ định lớp Internet.
- AAAA là loại bản ghi.
- 2001:0db8:85a3:0000:0000:8a2e:0370:7334 là địa chỉ IPv6 được ánh xạ tới www.

1.5. Bản ghi CNAME

Bản ghi CNAME được chuẩn hóa trong RFC 1035 và được sử dụng để định nghĩa một bí danh (alias) cho một máy chủ hoặc tên miền hiện được định nghĩa bởi một bản ghi A (Address Record).

Cấu trúc của bản ghi CNAME như sau:

```
<Tên miền bí danh> <class> <ttl> CNAME <tên miền>
```

Ví dụ:

```
web.vnnic.vn. IN CNAME www.vnnic.vn.
```

CÚ PHÁP	VÍ DỤ SỬ DỤNG	MÔ TẢ
name	web	web.vnnic.vn.
ttl		Không có TTL nào được định nghĩa cho bản ghi, TTL mặc định của tệp zone sẽ được sử dụng.
class	IN	Xác định lớp là Internet.
canonical-name	www.vnnic.vn.	Định nghĩa rằng www.vnnic.vn. là bí danh (alias) cho máy chủ hoặc tên miền web.vnnic.vn.

Bản ghi CNAME thường được sử dụng khi gán bí danh (alias) cho các dịch vụ. Ví dụ, nếu một máy chủ được đặt tên là bill và vận hành cả dịch vụ ftp lẫn web, bản ghi CNAME được sử dụng như sau:

```
ftp  IN  CNAME  bill
www  IN  CNAME  bill
bill IN  A      192.168.254.21
```

Bản ghi CNAME có một số điểm lưu ý và hạn chế như sau:

- Không sử dụng CNAME và NS hoặc MX cho cùng một tên miền. Cụ thể: một tên miền có bản ghi CNAME, thì không thể có bản ghi NS cho cùng một tên miền đó. Khai báo này có thể gây nhầm lẫn trong việc xác định máy chủ DNS nào chịu trách nhiệm cho tên miền. Tương tự, nếu một tên miền có bản ghi CNAME, thì không thể có bản ghi MX. Khai báo này có thể gây ra vấn đề trong việc gửi và nhận email, vì máy chủ mail sẽ không thể xác định được địa chỉ đúng để gửi thư.
- CNAME loop: Nếu có nhiều bản ghi CNAME trỏ lẫn nhau, có thể xảy ra vòng lặp CNAME, dẫn đến lỗi trong phân giải tên miền.
- Tăng độ trễ: Việc sử dụng bản ghi CNAME có thể làm tăng độ trễ trong quá trình phân giải tên miền, vì trình phân giải DNS phải thực hiện thêm một truy vấn đến tên miền chính.
- Một số dịch vụ và ứng dụng không hỗ trợ hoặc không hoạt động tốt với bản ghi CNAME, đặc biệt là khi cần cấu hình với các bản ghi khác.

1.6. Bản ghi MX

Bản ghi MX (Mail Exchange Record) được sử dụng để chỉ định máy chủ thư điện tử chịu trách nhiệm nhận email cho một tên miền cụ thể. Bản ghi MX được định nghĩa trong RFC 1035 và RFC 5321. Nó là một phần không thể thiếu trong việc cấu hình email cho các tổ chức và tên miền.

Cú pháp cơ bản của bản ghi MX như sau:

```
name  ttl  class  rr  preference  exchange
```

Ví dụ:

```
vnnic.vn.  IN  MX  10  mail1.vnnic.vn.
vnnic.vn.  IN  MX  20  mail2.vnnic.vn.
```

Trong ví dụ này:

- vnnic.vn. là tên miền.
- 10 và 20 là mức độ ưu tiên (priority), giá trị thấp hơn được ưu tiên cao hơn.
- mail1.vnnic.vn. và mail2.vnnic.vn. là các máy chủ thư điện tử.

- **Bản ghi MX được sử dụng để:**

- Xác định máy chủ nhận email cho một tên miền.
- Cung cấp hệ thống dự phòng cho dịch vụ email bằng cách chỉ định nhiều máy chủ với mức ưu tiên khác nhau.

- **Lưu ý khi sử dụng bản ghi MX:**

- Đảm bảo các máy chủ được chỉ định trong bản ghi MX có bản ghi A hoặc AAAA tương ứng. Không sử dụng CNAME trong bản ghi MX.
- Xác định mức độ ưu tiên rõ ràng để tối ưu hóa luồng email và đảm bảo tính sẵn sàng cao.
- Đảm bảo rằng máy chủ thư có cấu hình SPF, DKIM và DMARC để tăng cường bảo mật email.

1.7. Bản ghi TXT

Bản ghi TXT (Text Record) cho phép lưu trữ thông tin văn bản trong DNS. Ban đầu, bản ghi này được thiết kế để lưu trữ các ghi chú tùy ý, nhưng hiện tại nó được sử dụng rộng rãi trong các hệ thống xác thực email và bảo mật. Bản ghi TXT được định nghĩa trong RFC 1035.

Cú pháp cơ bản của bản ghi TXT như sau:

```
name  ttl  class  rr  text
```

Ví dụ:

```
vnnic.vn.  IN  TXT  "v=spf1 include:_spf.vnnic.vn ~all"
```

Trong đó:

- vnnic.vn. là tên miền.
- TXT là loại bản ghi.
- "v=spf1 include: spf.vnnic.vn ~all" là nội dung văn bản, trong trường hợp này dùng để cấu hình SPF (Sender Policy Framework).

- **Bản ghi TXT thường được sử dụng trong:**
- Xác thực email thông qua SPF, DKIM, và DMARC để ngăn chặn giả mạo email.
- Lưu trữ các thông tin tùy ý phục vụ các dịch vụ hoặc ứng dụng cụ thể.
- Quản lý và cấu hình dịch vụ trên các nền tảng đám mây.

- **Lưu ý khi sử dụng bản ghi TXT:**
- Nội dung văn bản trong bản ghi TXT không được vượt quá 255 ký tự trong mỗi chuỗi. Nếu dài hơn, cần chia thành nhiều chuỗi.
- Cần cấu hình chính xác các bản ghi TXT cho SPF, DKIM, và DMARC để tránh gây lỗi trong hệ thống email.
- Đảm bảo không sử dụng thông tin nhạy cảm hoặc bảo mật trong bản ghi TXT vì nội dung này công khai và dễ bị khai thác.

2. Các bản ghi khác

2.1. Bản ghi HTTPS/SVCB

Bản ghi HTTPS/SVCB là một cải tiến mới trong hệ thống DNS, được định nghĩa trong RFC 8499 và RFC 9221. Đây là các bản ghi thiết kế để tối ưu hóa việc định tuyến và cải thiện hiệu suất cho các dịch vụ mạng, đặc biệt là các dịch vụ web. Bản ghi SVCB đóng vai trò như một bản ghi "Service Binding", cung cấp thông tin chi tiết về dịch vụ như giao thức, cổng và các tham số liên quan. Bản ghi HTTPS, một trường hợp đặc biệt của SVCB, tập trung vào các dịch vụ web sử dụng giao thức HTTPS và hỗ trợ các giao thức hiện đại như HTTP/3.

Cú pháp:

```
<tên miền> <giá trị ưu tiên> <đích đến> <các tham số bổ sung>
```

Ví dụ:

```
vnnic.vn. 1 svc.vnnic.vn. alpn=h3 port=443
```

Trong đó, alpn=h3 chỉ định dịch vụ hỗ trợ giao thức HTTP/3 và port=443 chỉ ra rằng dịch vụ đang hoạt động trên cổng 443.

Bản ghi HTTPS/SVCB thường được sử dụng trong các trường hợp cần cải thiện hiệu suất kết nối mạng, tối ưu hóa độ trễ hoặc hỗ trợ các giao thức mới. Ví dụ, bản ghi này rất hữu ích trong các hệ thống CDN hoặc các dịch vụ web yêu cầu tải nhanh và bảo mật cao.

Cần lưu ý đảm bảo cả máy chủ DNS và ứng dụng đều hỗ trợ bản ghi này. Ngoài ra, cần duy trì tính tương thích với các hệ thống không hỗ trợ HTTPS/SVCB thông qua các bản ghi truyền thống như A hoặc AAAA.

2.2. Bản ghi CAA

Bản ghi CAA (Certification Authority Authorization) được định nghĩa trong RFC 8659 và được thiết kế để tăng cường bảo mật trong quá trình cấp phát chứng chỉ SSL/TLS. Nó cho phép chủ sở hữu tên miền xác định rõ các tổ chức cấp CA được phép phát hành chứng chỉ cho tên miền đó, từ đó ngăn chặn việc phát hành trái phép.

Cú pháp:

```
<tên miền> <cờ> <thẻ> <giá trị>
```

Ví dụ:

```
vnnic.vn. IN CAA 0 issue "letsencrypt.org"
```

Khai báo này chỉ định rằng chỉ có Let's Encrypt được phép phát hành chứng chỉ cho vnnic.vn.

Bản ghi CAA thường được sử dụng để kiểm soát và tăng cường bảo mật cho việc cấp phát chứng chỉ SSL/TLS, đặc biệt trong các hệ thống yêu cầu bảo mật cao. Đây là công cụ hữu ích trong việc giảm nguy cơ bị giả mạo chứng chỉ hoặc bị tấn công liên quan đến chứng chỉ.

Một số lưu ý khi sử dụng bản ghi CAA là đảm bảo rằng tất cả các CA cần thiết đều được liệt kê trong cấu hình. Đồng thời, cần kiểm tra tính tương thích với chính sách bảo mật hiện tại của doanh nghiệp và lưu ý rằng bản ghi này không áp dụng cho các chứng chỉ tự ký (self-signed).

2.3. Bản ghi SRV

Bản ghi SRV (Service Record), được định nghĩa trong RFC 2782, là một loại bản ghi DNS dùng để xác định vị trí các dịch vụ mạng, chẳng hạn như máy chủ và cổng cho một dịch vụ cụ thể. Bản ghi này thường được sử dụng trong các hệ thống như VoIP, XMPP hoặc Active Directory để cung cấp thông tin định tuyến.

Cú pháp:

```
<tên dịch vụ> <giao thức> <ưu tiên> <trọng số> <cổng> <tên máy chủ>
```

Ví dụ:

```
_sip._tcp.vnnic.vn. IN SRV 10 60 5060 sipserver.vnnic.vn.
```

Dòng này chỉ định dịch vụ SIP sử dụng giao thức TCP, với ưu tiên 10, trọng số 60, hoạt động trên cổng 5060 và được lưu trữ tại máy chủ sipserver.vnnic.vn.

Bản ghi SRV thường được sử dụng để định tuyến các dịch vụ mạng trong các hệ thống phức tạp có nhiều máy chủ. Nó cũng hữu ích trong các hệ thống cần dự phòng hoặc cân bằng tải.

Khi sử dụng bản ghi SRV, cần đảm bảo rằng các dịch vụ liên quan được cấu hình đúng để sử dụng thông tin từ bản ghi. Đồng thời, cần kiểm tra tính tương thích của các ứng dụng khách, vì không phải tất cả các ứng dụng đều hỗ trợ bản ghi SRV.

VIII

DNS VÀ IPv6

1. Ánh xạ tên miền và địa chỉ IPv6

Hiện nay việc ánh xạ tên miền và địa chỉ IPv4 thông qua bản ghi A, tuy nhiên bản ghi A không được xây dựng để hỗ trợ địa chỉ IPv6 với 128 bits địa chỉ. Hệ thống DNS hỗ trợ IPv6 từ năm 1995 thông qua RFC 1886, 3596; RFC này đề cập đến một số vấn đề cơ bản như sau:

- Ánh xạ tên miền vào địa chỉ IPv6 thông qua bản ghi AAAA
- Ánh xạ địa chỉ IPv6 sang tên miền sử dụng miền ip6.arpa.
- Ánh xạ địa chỉ IPv6 sang tên miền sử dụng bản ghi PTR.

- **Phân giải tên miền thuận trong IPv6:**

Để ánh xạ một tên miền tới địa chỉ IPv6, hệ thống tên miền sử dụng kiểu bản ghi mới, gọi là bản ghi AAAA (tương đương bản ghi kiểu A trong địa chỉ IPv4). Bản ghi AAAA có dạng thức như sau:

```
www.abc.test    AAAA   3FFE:B00:C18:1::2
```

- **Phân giải tên miền ngược trong IPv6, bản ghi PTR:**

Để ánh xạ địa chỉ IPv6 tới tên miền, hệ thống DNS cũng sử dụng kiểu bản ghi PTR, việc khai báo tên miền ngược cho tên miền khai báo ở trên như sau:

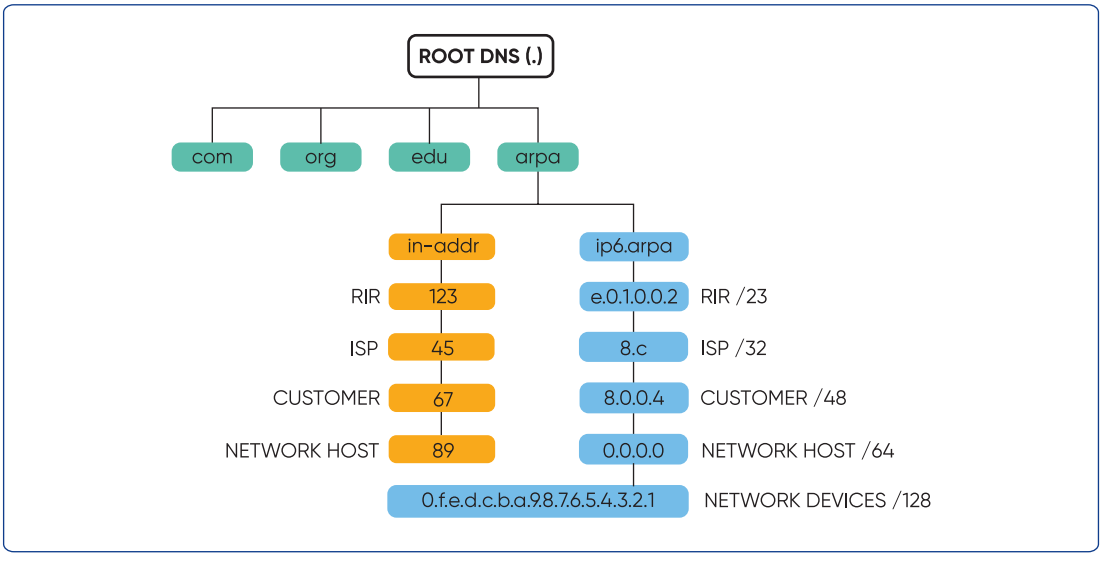
```
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.0.0.b.0.e.f.f.3.ip6.arpa PTR www.abc.test
```

Địa chỉ IPv4 sử dụng miền ".in-addr.arpa" cho tên miền ngược. Tên miền ngược cho địa chỉ IPv4 được chuyển giao dạng classful (/8/16 và /24).

Ban đầu, RFC 1886 sử dụng miền ".ip6.int" để khai báo tên miền ngược, sau này miền ".ip6.int" được hủy bỏ. Tên miền ngược IPv6 được khai báo và chuyển giao trong không gian tên miền ".ip6.arpa" của hệ thống tên miền toàn cầu.

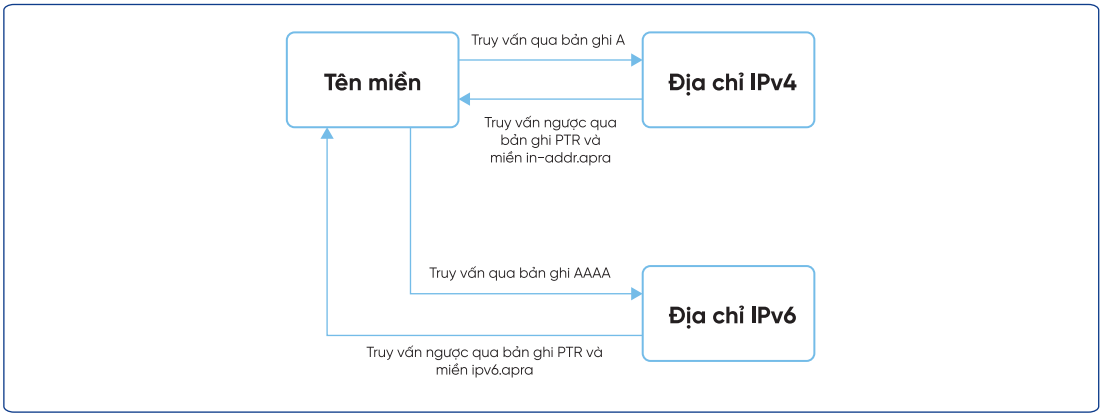
Địa chỉ IPv6 hoàn toàn là dạng thức classless, không còn tồn tại khái niệm classful. Địa chỉ IPv6 được biểu diễn gồm 32 chữ số hexa (mỗi số hexa tương ứng 4 bit). Tên miền ngược tương ứng địa chỉ IPv6 được chuyển giao theo các biên 4 bit đó.

Hình dưới đây thể hiện việc khai báo tên miền ngược trong IPv4 và IPv6, cả hai đều được khai báo dưới miền arpa trong không gian tên miền.



Hình 19: Khai báo tên miền ngược IPv6

Hình dưới đây tổng thể hiện quá trình truy vấn tên miền thuận và ngược trong IPv4 và IPv6.



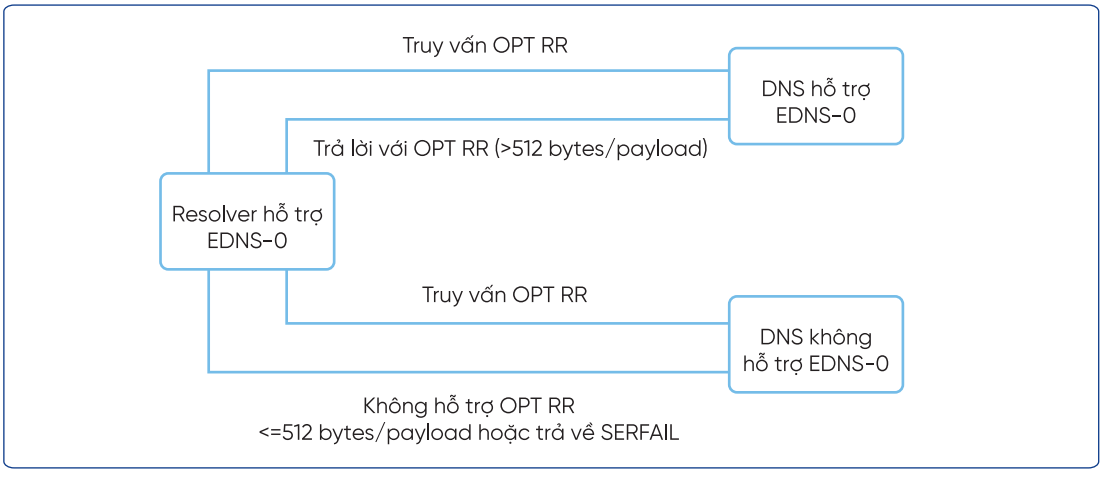
Hình 20: Truy vấn trên hệ thống DNS IPv4, IPv6

2. Giao thức truyền tải trong mạng DNS IPv6

Giao thức truyền tải DNS trong mạng IPv6 vẫn được giữ nguyên là UDP/53 và TCP/53, quá trình truy vấn tên miền trong mạng thuần IPv6 hoàn toàn giống trong mạng IPv4, điểm khác biệt duy nhất ở đây là trường địa chỉ IP trong bản tin truy vấn và trả lời là địa chỉ IPv6 128 bit, điều này làm tăng tải xử lý và truyền dẫn trên mạng so với truy vấn địa chỉ IPv4.

Bản tin truy vấn tên miền qua giao thức UDP bị giới hạn trong 512 byte, khi chuyển sang địa chỉ IPv6 thì giới hạn này có thể bị vượt qua, nếu tiếp tục tuân theo nguyên tắc hoạt động của DNS trong IPv4 thì trường hợp này hệ thống sẽ sử dụng giao thức TCP làm giao thức truyền tải thay vì UDP.

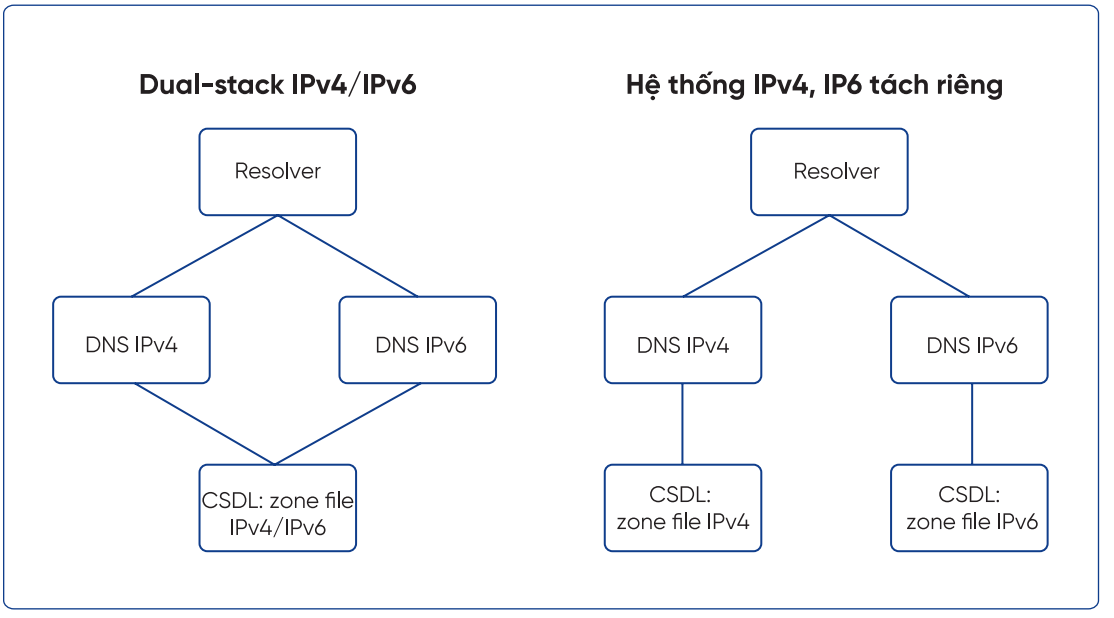
Để giải quyết các vấn đề giới hạn của hệ thống DNS, một RFC được xây dựng là RFC 2671 (Extension Mechanisms for DNS - EDNS0), RFC này đưa ra phương án giải quyết giới hạn 512 byte bằng cách bổ sung một bản ghi pseudo gọi là OPT. Nguyên tắc hoạt động là DNS Resolver và DNS server trao đổi thông tin về số lượng byte tối đa có thể sử dụng thông qua bản ghi OPT, từ đó có thể thực hiện các truy vấn quá 512 byte.



Hình 21: Cơ chế mở rộng DNS cho IPv6

Hiện nay hầu hết các phiên bản phần mềm DNS đã được cập nhật, nâng cấp để hỗ trợ RFC 2671 như BIND, NSD, Knot, DNS của Windows, ...

- Dữ liệu truyền tải trong mạng DNS IPv6: Khi triển khai DNS để hỗ trợ IPv6, có hai cách tiếp cận:
+ Xem xét DNS như một cơ sở dữ liệu (CSDL), bao gồm cả các bản ghi cho IPv4 và IPv6: SOA, NS, A, AAAA, MX, PTR, TXT. Khi đó CSDL này hoàn toàn độc lập với giao thức truyền tải IP là IPv4 hay IPv6.
+ Xem xét DNS như là một chương trình ứng dụng TCP/IP: Như vậy dịch vụ DNS có thể được truy cập từ mạng IPv4 hoặc IPv6. Khi đó CSDL tên miền phải được đồng bộ đảm bảo thông tin trả lời phải chính xác, cách tiếp cận này có thể gây ra việc một số bản ghi không thể truy vấn được ở mạng IPv4 nhưng lại có thể truy vấn từ mạng IPv6 do mất đồng bộ dữ liệu.



Hình 22: Các phương thức triển khai DNS với IPv6

Tổ chức, cá nhân khi triển khai DNS của mình trên mạng IPv6 cần tuân thủ theo hai RFC là:

- RFC 3901: "DNS IPv6 Transport Operational Guidelines".
- RFC 4472: "Operational Considerations and Issues with IPv6".

Hai RFC này hướng dẫn triển khai DNS và các vấn đề gặp phải trong quá trình triển khai, có thể tổng kết lại như sau:

- Bất kỳ DNS zone nào nên được quản lý bởi ít nhất một DNS IPv4.
- Các DNS đệ quy nên được triển khai trên mạng IPv4 hoặc dual-stack (cả IPv4 và IPv6).
- Tất cả các zone nên được truy xuất qua cả mạng IPv4 và IPv6

Hiện nay, hầu hết các chương trình, phần mềm máy chủ DNS đều đã nâng cấp nhằm hỗ trợ địa chỉ IPv6.

PHẦN MỀM	HỖ TRỢ IPv6
BIND	Đã hỗ trợ IPv6 từ phiên bản BIND 9.x
PowerDNS	Đã hỗ trợ IPv6 từ phiên bản 3.0
CoreDNS	Đã hỗ trợ IPv6
Unbound	Đã hỗ trợ IPv6
NSD	Đã hỗ trợ IPv6
Knot DNS	Đã hỗ trợ IPv6
Microsoft DNS	Đã hỗ trợ từ phiên bản Windows Server 2003 trở lên

IX

CÀI ĐẶT VÀ TỐI ƯU DNS

Hiện nay có nhiều phần mềm máy chủ DNS như BIND, PowerDNS, Microsoft DNS, ... Trong đó, phần mềm BIND (Berkeley Internet Name Domain) là một trong những phần mềm DNS phổ biến nhất. Với các tính năng như sau:

- Hỗ trợ rộng rãi: Là một phần mềm mã nguồn mở, BIND được hỗ trợ và phát triển bởi nhiều cộng đồng và tổ chức, giúp cải thiện tính ổn định và bảo mật.
- Tính tương thích cao: BIND có khả năng tương thích với nhiều loại hệ thống và phần mềm khác nhau, làm cho nó trở thành sự lựa chọn phổ biến cho các máy chủ DNS.
- Chức năng toàn diện: BIND cung cấp đầy đủ các chức năng của một máy chủ DNS, bao gồm hỗ trợ cho cả DNS chính (master) và phụ (slave), cũng như khả năng quản lý nhiều zone tên miền.
- Tính linh hoạt: BIND cho phép cấu hình rất linh hoạt, từ việc quản lý các bản ghi DNS đơn giản cho đến các cấu hình phức tạp với nhiều zone tên miền và chính sách truy cập.
- Cộng đồng và tài liệu phong phú: Với một cộng đồng lớn và tài liệu hướng dẫn chi tiết, người dùng có thể dễ dàng tìm kiếm sự trợ giúp và giải pháp cho các vấn đề gặp phải.
- Bảo mật: BIND liên tục được cập nhật để khắc phục các vấn đề bảo mật, giúp bảo vệ hệ thống DNS khỏi các mối đe dọa từ bên ngoài.

Vì vậy, trong tài liệu này sẽ tập trung hướng dẫn cài đặt máy chủ DNS sử dụng phần mềm BIND, trên môi trường hệ điều hành Unix/Linux (như CentOS, Ubuntu, Debian, Redhat Linux, ...). Để có thể cài đặt được máy chủ DNS cần có các kiến thức và biết sử dụng được các lệnh trong hệ điều hành Unix/Linux.

1. Cài đặt máy chủ DNS

1.1. Chuẩn bị môi trường

Trước khi cài đặt BIND9 từ mã nguồn, chúng ta cần đảm bảo rằng hệ thống có đầy đủ công cụ biên dịch và thư viện cần thiết.

1.1.1. Cập nhật hệ thống

```
• Ubuntu/Debian:
# sudo apt update && sudo apt upgrade -y
• CentOS/RHEL:
# sudo yum update -y
```

1.1.2. Cài đặt các gói phụ thuộc

```
Để biên dịch BIND9 từ mã nguồn, chúng ta cần cài đặt các công cụ và thư viện bắt buộc.
• Ubuntu/Debian:
# sudo apt install build-essential libssl-dev libuv1-dev libcap-dev libjson-c-dev libxml2-dev libtool flex
bison git pkg-config -y
• CentOS/RHEL:
# sudo yum groupinstall “Development Tools” -y
# sudo yum install openssl-devel libuv-devel libcap-devel json-c-devel libxml2-devel libtool flex bison
git pkgconf -y
```

1.2. Tải xuống mã nguồn BIND9

Mã nguồn BIND9 có thể tải từ trang web chính thức của ISC (Internet Systems Consortium) hoặc từ GitHub.

1.2.1. Tải phiên bản mới nhất từ ISC

```
# wget https://downloads.isc.org/isc/bind9/9.18.12/bind-9.18.12.tar.gz
(Thay thế phiên bản mới nhất tại https://downloads.isc.org/isc/bind9/)
```

1.2.2. Hoặc tải từ GitHub

```
# git clone https://gitlab.isc.org/isc-projects/bind9.
```

1.3. Giải nén và biên dịch BIND9

1.3.1. Giải nén mã nguồn

```
# tar -xvzf bind-9.18.12.tar.gz
# cd bind-9.18.12
```

1.3.2. Cấu hình trước khi biên dịch

```
# ./configure --prefix=/usr/local/bind9 \
        --sysconfdir=/etc/bind9 \
        --localstatedir=/var/bind9 \
        --enable-threads \
        --enable-largefile \
        --with-openssl \
        --with-libjson \
        --with-libxml2
```

Giải thích các tham số cấu hình:

```
# Cài đặt BIND9 vào thư mục /usr/local/bind9:
--prefix=/usr/local/bind9
# Lưu trữ file cấu hình tại /etc/bind9:
--sysconfdir=/etc/bind9
# Hỗ trợ DNSSEC và TLS:
--with-openssl
# Bật hỗ trợ đa luồng (multi-threading):
--enable-threads
```

1.3.3. Biên dịch BIND9

```
# make -j$(nproc)
(Sử dụng -j$(nproc) để tận dụng tất cả các lõi (core) CPU giúp biên dịch nhanh hơn.)
```

1.3.4. Cài đặt BIND9

```
# make install
```

1.4. Cấu hình hệ thống để sử dụng BIND9:

Sau khi cài đặt, chúng ta cần cấu hình BIND9 như một dịch vụ hệ thống (systemd).

1.4.1. Tạo tài khoản và thư mục cho BIND9

```
# sudo mkdir -p /var/bind9 /etc/bind9 /var/log/bind9
# sudo useradd -r -d /var/bind9 -s /bin/false named
# sudo groupadd named
# usermod -aG named named
# sudo chown -R named:named /var/bind9 /etc/bind9 /var/log/bind9
```

1.4.2. Tạo file dịch vụ systemd

```
# sudo nano /etc/systemd/system/named.service
```

- Thêm nội dung sau:

```
[Unit]
Description=BIND 9 DNS server
After=network.target

[Service]
ExecStart=/usr/local/bind9/sbin/named -u named -c /etc/bind9/named.conf
ExecReload=/bin/kill -HUP $MAINPID
Restart=always
User=named
Group=named
```

- Lưu file và tải lại systemd:

```
# sudo systemctl daemon-reload
# sudo systemctl enable named
```

1.5. Cấu hình cơ bản

1.5.1. Cấu hình máy chủ DNS Caching

```
# sudo nano /etc/bind9/named.conf.options
```

- Thêm nội dung:

```
options {
directory "/var/bind9"; # Thư mục chứa các tệp cấu hình và dữ liệu
recursion yes; # Bật tính năng đệ quy
allow-recursion { ip_address; }; # Cho phép các yêu cầu đệ quy từ mạng nội bộ
listen-on port 53 { any; }; # Lắng nghe trên cổng 53 trên mọi địa chỉ
dnssec-validation auto; # Tự động xác thực DNSSEC
};
```

- Khởi động lại BIND9:

```
# sudo systemctl restart named
# sudo systemctl status named
```

1.5.2. Cấu hình máy chủ Authoritative DNS Server

Authoritative DNS Server là máy chủ chính thức chịu trách nhiệm cung cấp thông tin của một tên miền cụ thể. Nó lưu trữ và trả lời các truy vấn về bản ghi DNS của tên miền đó. Thông thường mô hình triển khai gồm 02 máy chủ:

- Primary DNS Server (Master Server): Máy chủ chính, quản lý và cập nhật thông tin về tên miền.
- Secondary DNS Server (Slave Server): Máy chủ phụ, sao chép dữ liệu từ máy chủ chính để đảm bảo dự phòng.

a) Cấu hình Primary DNS Server (Master DNS Server):

- Chỉnh sửa file cấu hình named.conf.local để khai báo zone tên miền:

```
# sudo nano /etc/bind/named.conf.local
```

- Thêm cấu hình cho tên miền vnnic.vn:

```
zone "vnnic.vn" {
    type master;
    file "/etc/bind/db.vnnic.vn";
};
```

- Tạo file zone cho tên miền vnnic.vn

```
# sudo nano /etc/bind/db.vnnic.vn
```

- Thêm nội dung:

```
$TTL 86400
@   IN  SOA     ns1.vnnic.vn. admin.vnnic.vn. (
              2024031401  ; Serial number
              3600        ; Refresh
              1800        ; Retry
              604800      ; Expire
              86400       ; Minimum TTL
)
@       IN  NS      ns1.vnnic.vn.         ; Khai báo máy chủ DNS chính cho miền
@       IN  A       192.168.1.100         ; Địa chỉ IP cho miền gốc
ns1     IN  A       192.168.1.100         ; Địa chỉ IP cho máy chủ DNS ns1
www     IN  A       192.168.1.101         ; Địa chỉ IP cho máy chủ www
mail    IN  A       192.168.1.102         ; Địa chỉ IP cho máy chủ mail
@       IN  MX  10  mail.vnnic.vn.    ; Khai báo máy chủ nhận email với độ ưu tiên 10
```

- Kiểm tra cấu hình BIND9

```
# sudo named-checkconf
# sudo named-checkzone vnnic.vn /etc/bind/db.vnnic.vn
```

- Nếu không có lỗi, khởi động lại BIND9:

```
# sudo systemctl restart named
# sudo systemctl enable named
```

b) Cấu hình Secondary DNS Server (Slave DNS Server):

- Chỉnh sửa file cấu hình:
  Mở named.conf.local trên máy chủ Slave:

```
# sudo nano /etc/bind/named.conf.local
```

- Thêm cấu hình:

```
zone "vnnic.vn" {
    type slave;
    masters { 192.168.1.100; };
    file "/var/cache/bind/db.vnnic.vn";
};
```

- Kiểm tra cấu hình BIND9

```
# sudo named-checkconf
```

- Khởi động lại BIND9

```
# sudo systemctl restart named
# sudo systemctl enable named
```

2. Tối ưu DNS

2.1. Cấu hình dữ liệu

Việc tùy chỉnh trong cấu hình dữ liệu, có thể giúp tối ưu hóa hiệu suất, bảo mật và tính khả dụng của dịch vụ DNS. Trong đó tập trung vào điều chỉnh các bản ghi, tham số một cách phù hợp nhất, đặc biệt là các tham số giá trị TTL. TTL là thời gian tồn tại (cache) bản ghi DNS trên các máy chủ phân giải DNS đệ quy. Việc đặt giá trị TTL hợp lý rất quan trọng:

- TTL quá dài (ví dụ 24 giờ hoặc hơn) khiến việc thay đổi bản ghi chậm được cập nhật, ảnh hưởng việc chuyển đổi dịch vụ.
- TTL quá ngắn (< 300 giây) làm tăng tải cho hệ thống DNS, vì phải xử lý quá nhiều truy vấn mới và tăng độ trễ cho người dùng.
- - TTL lý tưởng cho dịch vụ web thông thường khoảng 3600 giây (1 giờ). Khi sắp thay đổi cấu hình DNS, nên giảm TTL dần dần xuống (600s hoặc 300s) vài ngày trước đó để đảm bảo cập nhật nhanh chóng.

Các tham số tiêu chuẩn, khuyến nghị sử dụng khai báo cho các bản ghi DNS như sau:

STT	ĐỐI TƯỢNG	THAM SỐ CHI TIẾT	THÔNG SỐ YÊU CẦU, KHUYẾN NGHỊ	TIÊU CHUẨN, SỞ CỨ
1	Bản ghi SOA			RFC 1033
		Refresh	3600 (s)	
		Retry	600 (s)	
		Expire	360000 (s)	
		Minimum	86400 (s)	
				RFC 1912
		Refresh	2 giờ - 3 giờ (3600 - 7200)	
		Retry	Nhỏ hơn Refresh Time (120 - 7200)	
		Expire	2 - 4 tuần (1209600 - 2419200)	
		Minimum	1 - 5 ngày (86400 - 432000)	
2	Giá trị TTL			
		TTL		RFC 1033; RFC 2308
			1 ngày - 1 tuần (86400 - 604800)	
			1 giờ - 1 ngày (3600 - 86400)	
3	Bản ghi NS			
		NS	Tối thiểu phải khai báo 02 bản ghi NS trỏ về 02 Nameservers khác nhau (01 Primary và 01 Secondary).	RFC 1537 RFC 1035
			Bản ghi NS phải tồn tại cả trong zone chuyển giao (child) và zone quản lý chính nó (apex zone).	RFC 1033
4	Bản ghi Glue record	NS, A/AAAA	Khai báo bản ghi NS kèm theo bản ghi A hoặc AAAA.	RFC 1033
5	Bản ghi MX	- Priority - Hostname - Bản ghi A/AAAA của Hostname	Khi khai báo 01 bản ghi MX thì phải khai bảo bản ghi A/AAAA tương ứng cho hostname của bản ghi MX đó.	
6	Bản ghi CNAME	- Hostname được trỏ CNAME - Bản ghi A/AAAA của Hostname được trỏ CNAME	Khi khai báo 01 bản ghi CNAME thì phải khai bảo bản ghi A/AAAA tương ứng cho hostname của bản ghi CNAME đó.	

2.2. Cấu hình dịch vụ DNS

2.2.1. Giới hạn các chức năng (Limit Functionality)

Để giảm thiểu các nguy cơ, rủi ro về an toàn thông tin cần hạn chế tối đa sử dụng các tiến trình dễ bị khai thác. Ví dụ, bằng cách sử dụng nhiều máy chủ chính (multiple masters), có thể thiết lập hệ thống mà không cần thực hiện đồng bộ dữ liệu (zone transfer). Trong trường hợp này do chỉ có các máy chủ chính mà không có các máy chủ phụ nên các câu lệnh allow-transfer và notify có thể được thiết lập thành "none" trong phần tùy chọn toàn cục (global options clause).

(1) Cấu hình phòng ngừa rủi ro (Defensive Configuration)

Là khai báo mà trong đó tất cả các tính năng quan trọng, đặc biệt là những tính năng liên quan đến bảo mật, đều được định nghĩa rõ là BẬT hoặc TẮT. Khai báo này sẽ vô hiệu hóa các cấu hình mặc định có sẵn và thiết lập yêu cầu cụ thể (bật hay tắt), bằng cách sử dụng các lệnh khai báo với tham số phù hợp.

Các cấu hình mặc định của phần mềm thường rất thuận tiện, tuy nhiên lại tiềm ẩn nhiều vấn đề rủi ro, dễ bị khai thác. Ví dụ, theo mặc định phiên bản hiện tại của BIND vô hiệu hóa chức năng Dynamic DNS (DDNS). Tuy nhiên, để đảm bảo chức năng này không được sử dụng trong mọi trường hợp, thì cán bộ quản trị sẽ cấu hình để vô hiệu hóa chức năng mặc định này như sau:

```
allow-update {"none";};
```

(2) Nguyên tắc quản lý quyền truy cập

Áp dụng quy tắc Deny All, Allow Selectively (từ chối tất cả, chỉ cho phép có chọn lọc). Nguyên tắc này giúp hạn chế rủi ro bảo mật, chỉ cấp quyền cho các đối tượng thực sự cần thiết, đồng thời tránh tình trạng mở rộng quyền không cần thiết. Ví dụ khai báo để thiết lập cơ chế từ chối toàn bộ việc đồng bộ zone tên miền, nhưng vẫn cho phép một máy chủ cụ thể có thể thực hiện đồng bộ:

```
options {
   ....
   allow-transfer {none;};  // Không cho phép đồng bộ mặc định
   ....
};
zone "vnnic.vn" in {
   ....
   allow-transfer {10.0.1.2;};  // Chỉ cho phép máy chủ này đồng bộ
   ....
};
```

(3) Truy cập từ xa (remote access)

Các phiên bản BIND tích hợp sẵn công cụ quản trị có tên là RNDC (Remote Name Daemon Control), có thể được sử dụng cục bộ (localhost) hoặc từ xa (remote). Đây là công cụ quản trị thuận tiện, tuy nhiên vẫn có nguy cơ bị lợi dụng. Mặc định BIND chỉ cho phép rndc hoạt động từ địa chỉ localhost (127.0.0.1). Nếu không sử dụng rndc, khuyến nghị nên vô hiệu hóa công cụ này bằng cách sử dụng khai báo trường controls rỗng như sau:

```
// Cấu hình named.conf
controls {};
....
```

Nếu sử dụng RNDC, khuyến nghị khai báo trường controls cụ thể, ngay cả khi chỉ cho phép truy cập từ localhost, cụ thể như sau:

```
// Trích đoạn cấu hình named.conf
controls {
   inet 127.0.0.1 allow {localhost;} keys {"rndc-key"};
};
```

Trong đoạn cấu hình trên, rndc-key là tên khóa mặc định được tạo bởi lệnh:

```
# rndc-confgen -a
```

Các tệp cấu hình rndc.conf và các tệp chứa khóa như rndc.key là rất quan trọng đối với rndc và phải được bảo vệ với quyền truy cập hạn chế.

Để thiết lập rndc có thể kết nối, truy cập quản lý từ xa cần phải thiết lập các chính sách bảo mật chặt chẽ hơn như: thay đổi cổng kết nối mặc định, cấu hình ACL, thay đổi tên khóa bảo mật mặc định,...

Ví dụ dưới đây cho thấy rằng người dùng trên địa chỉ loopback (127.0.0.1) có thể sử dụng khóa mặc định để truy cập, trong khi tất cả các người dùng khác phải sử dụng khóa rndc-remote. Mặc định localhost sẽ sử dụng cổng 953 và cổng kết nối bên ngoài sẽ thay đổi và được thiết lập là 7766. Đồng thời áp dụng các điều khoản ACL (address_match_list) giới hạn, kiểm soát nguồn truy cập:

```
// named.conf fragment
acl "rndc-users" {
    10.0.15.0/24;
    !10.0.16.1/24;
    2001:db8:0:27::/64;
 };
....
key "rndc-remote" {
    algorithm hmac-md5;
    secret "OmItW1lOyLVUEuvv+Fme+Q==";
};
controls {
    // local host - default key
    inet 127.0.0.1 allow {localhost;};
    inet * port 7766 allow {"rndc-users";} keys {"rndc-remote";};
};
```

2.2.2. Giới hạn quyền truy cập (Limit Permissions)

Giới hạn quyền truy cập là việc hạn chế, kiểm soát các truy cập vào các tệp tin bảo mật mà phần mềm hoặc ứng dụng DNS sử dụng, nhằm đảm bảo các ứng dụng hoặc người dùng khác (không được cấp phép) không thể đọc hoặc ghi vào các tệp tin bảo mật này.

Dưới đây là các tệp tin quan trọng và phải được giới hạn quyền truy cập trong phần mềm BIND:

(1) Tệp tin named.conf

Tệp tin named.conf là một tệp tin quan trọng, vì nó chứa thông tin cấu hình quan trọng cho hoạt động của DNS, trong đó có các thông tin như địa chỉ IP, các chính sách bảo mật, khóa bảo mật, ... nếu bị lộ lọt thông tin có thể bị lợi dụng để thực hiện các cuộc tấn công giả mạo (spoofing) hoặc các cuộc tấn công khác.

- Theo chính sách bảo mật, tệp tin named.conf không bao giờ được chứa các thông tin cụ thể về khóa bảo mật, bao gồm cả khóa dùng cho truy cập rndc.
- Thay vào đó, các khóa bảo mật cần được lưu trữ trong tệp riêng biệt nằm trong thư mục riêng và được tham chiếu vào named.conf bằng lệnh include.
- Nếu sử dụng thiết lập tính năng "view" trong phần mềm BIND, tối thiểu các cấu hình chứa thông tin "nhạy cảm" cũng phải được đặt trong tệp riêng biệt và tham chiếu vào named.conf.

Nếu chính sách của tổ chức cho phép người dùng cuối hoặc nhiều người chỉnh sửa tệp named.conf, thì các phần có thể chỉnh sửa đó nên được lưu trữ trong thư mục riêng biệt với các quyền truy cập được kiểm soát trước khi kết hợp vào named.conf.

Lưu ý: Các cấu hình cho trusted-keys chỉ chứa khóa công khai (public keys) và không phải thông tin "nhạy cảm". Không giống như key clauses (chứa khóa bí mật), trusted-keys chỉ cần bảo vệ chống lại lỗi ghi đè (write corruption) thay vì ngăn chặn đọc trái phép.

(2) Tệp tin được tham chiếu (Included files)

Các tệp tin được tham chiếu từ named.conf có thể có các mức quyền truy cập khác nhau. Phương pháp kiểm soát truy cập tốt nhất là phân loại các tệp tin theo chức năng, sau đó đặt chúng vào các thư mục riêng, thay vì gán quyền truy cập trực tiếp trên từng tệp tin.

Ví dụ:

- Các tệp chứa khóa bảo mật có thể được lưu trong thư mục /var/named/keys.
- Các tệp chứa cấu hình view riêng tư có thể được lưu trong /var/named/views.
- Các tệp dữ liệu zone riêng tư có thể được đặt trong /var/named/zone-private.
- Các tệp dữ liệu zone có thể chỉnh sửa nên được đặt trong thư mục home của người dùng được cấp quyền chỉnh sửa.

(3) Dữ liệu zone (zone files)

Các tệp dữ liệu zone thường chứa thông tin về các bản ghi DNS và được công khai, do đó việc bảo vệ chúng chủ yếu là kiểm soát quyền ghi (write permissions). Nếu hệ thống máy chủ DNS sử dụng cấu hình dựa trên chức năng "view", các tệp dữ liệu zone có thể chứa dữ liệu "nhạy cảm" và cần các cơ chế bảo vệ riêng biệt. Cách tối ưu nhất là phân tách zone chứa dữ liệu "nhạy cảm" vào một thư mục riêng, ví dụ:

- /var/named/master/private (chứa các tệp dữ liệu zone có chứa dữ liệu "nhạy cảm").
- /var/named/master/public (chứa các tệp dữ liệu zone công khai).
- /var/named/slave (chứa các tệp dữ liệu zone slave, yêu cầu quyền ghi cho BIND).

(4) Tệp tin PID (PID file)

Tệp tin này thường được ghi vào /var/run/named.pid hoặc /var/run/named/named.pid. Mặc dù nó chứa thông tin nhạy cảm (Process Identifier - PID của tiến trình named daemon), nhưng thông tin này chỉ có thể được sử dụng bởi tài khoản root. Nếu hệ thống bị khai thác lỗ hổng quyền root (root exploit), các tệp PID thường không phải là mối đe dọa an toàn an ninh cho hệ thống DNS. Tệp PID cần quyền ghi (write access) cho BIND và quyền đọc (read access) cho các script sử dụng nó để thực hiện các thao tác như khởi động, dừng, khởi động lại (start, stop, restart, v.v.).

(5) Tệp tin nhật ký (Log files)

Mặc định, các tệp tin nhật ký (log) để được ghi vào thư mục /var/log/named, chủ yếu là để thuận tiện chứ không phải vì lý do bảo mật. Về tổng thể, tệp nhật ký không chứa thông tin nhạy cảm và không yêu cầu biện pháp xử lý đặc biệt. Tuy nhiên, nếu cấu hình "view" được sử dụng trong chế độ stealth configuration (cấu hình ẩn), thì nhật ký có thể chứa thông tin nhạy cảm về địa chỉ IP riêng tư. Do đó, tùy thuộc vào thiết lập logging, các tệp nhật ký cần được bảo vệ để tránh rò rỉ thông tin quan trọng. Chi tiết các cấu hình logging trong mục X. Các công cụ hỗ trợ quản lý, vận hành.

(6) Tệp tin rndc (rndc files)

Như đã đề cập ở phần trên, các tệp tin cấu hình rndc.conf và các tệp tin chứa khóa như rndc.key là rất quan trọng đối với RNDC, cần được bảo vệ và hạn chế các quyền truy cập.

(7) Tệp tin nhật ký tạm (Journal files)

Theo cơ chế của BIND, một tệp dữ liệu zone (zone file) thường chỉ đọc. Nếu cập nhật động (Dynamic Update - DDNS) được sử dụng, các bản cập nhật sẽ được ghi vào một tệp nhị phân có đuôi định dạng .jnl cho từng zone tên miền và chỉ định kỳ được ghi vào tệp dữ liệu zone. Đối với các tệp dữ liệu zone công khai (public zone files), thông tin này không nhạy cảm. Tuy nhiên, với các tệp tin dữ liệu zone riêng tư (private zone files), cần phải đặt quyền hạn chặt chẽ.

X

CÁC CÔNG CỤ HỖ TRỢ QUẢN LÝ, VẬN HÀNH

1. Công cụ hỗ trợ cài đặt

Việc triển khai cài đặt phần mềm DNS, thông thường sẽ phụ thuộc vào đặc thù của mỗi loại phần mềm (PowerDNS, BIND, NSD, Unbound, ...), chức năng của máy chủ DNS (Authoritative hay Recursive Resolver, ...) và được triển khai trên hạ tầng, nền tảng hệ điều hành nào (Unix/Linux/Windows). Do đó, trong mỗi trường hợp sẽ có các bước triển khai cài đặt và bộ công cụ hỗ trợ cài đặt riêng. Trong nội dung này sẽ giới thiệu một số công cụ hỗ trợ cài đặt phần mềm BIND9 trên các hệ điều hành Unix/Linux (một trong những phần mềm DNS được sử dụng phổ biến nhất hiện nay) như sau:

1.1. Các công cụ hỗ trợ cài đặt từ gói cài đặt có sẵn:

1.1.1. Hệ điều hành Ubuntu/Debian:

APT (Advanced Package Tool) là công cụ quản lý gói mặc định được sử dụng rộng rãi trên các bản phân phối Linux dựa trên Debian, chẳng hạn như Debian, Ubuntu, Linux Mint và Kali Linux. APT sử dụng các file cấu hình để kết nối tới các kho lưu trữ (repositories), từ đó tải xuống và cài đặt các gói phần mềm cần thiết.

Cài đặt phần mềm BIND sử dụng công cụ APT:

```
# apt install bind9 bind9utils bind9-doc
```

1.1.2. Hệ điều hành Redhat/Centos

YUM là công cụ quản lý gói được sử dụng phổ biến trên các bản phân phối Linux thuộc họ Red Hat, bao gồm RHEL (Red Hat Enterprise Linux), CentOS, Fedora, Rocky Linux và AlmaLinux. Tương tự APT, YUM quản lý các gói phần mềm từ kho (repository) trực tuyến, hỗ trợ cài đặt, cập nhật, quản lý phiên bản phần mềm một cách đơn giản và hiệu quả.

```
# yum install bind bind-utils bind-chroot
```

1.2. Các công cụ hỗ trợ cài đặt từ mã nguồn (Source code):

Khi cài đặt phần mềm DNS (BIND) từ mã nguồn (Chi tiết các bước cài đặt, cấu hình được mô tả tại Mục VI) hệ thống yêu cầu sử dụng công cụ biên dịch mã nguồn, gọi là "make". MAKE là công cụ tự động giúp quản lý việc biên dịch và liên kết các tệp mã nguồn (source files) thành chương trình thực thi (executables) hoặc thư viện (libraries). Công cụ này dựa vào file có tên Makefile (hoặc makefile) – đây là file văn bản chứa các quy tắc (rules) và hướng dẫn chi tiết cách thức biên dịch các file nguồn.

```
# make
# make install
```

2. Công cụ hỗ trợ giám sát, kiểm tra sức khỏe

Hiện nay, các công cụ hỗ trợ giám sát, kiểm tra sức khỏe cho hệ thống, dịch vụ DNS được các chuyên gia, cộng đồng DNS sử dụng phổ biến như:

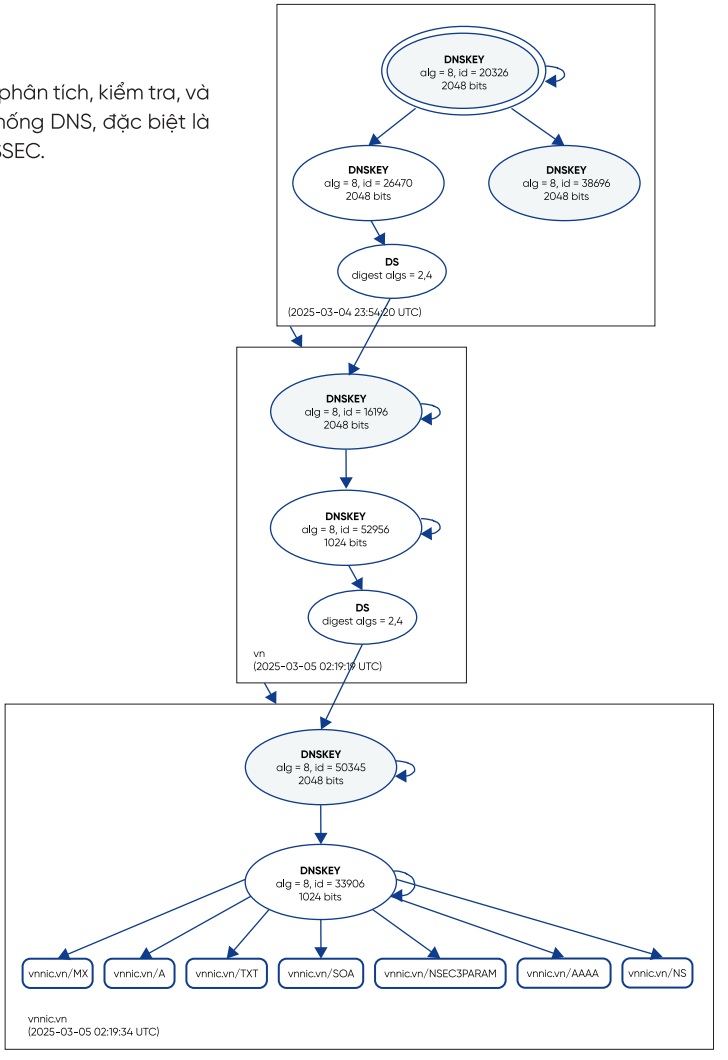
2.1. DNSChecker

- Địa chỉ: https://dnschecker.org/
- DNSChecker là một công cụ trực tuyến phổ biến, được sử dụng rộng rãi để kiểm tra và xác thực các bản ghi DNS trên phạm vi toàn cầu một cách nhanh chóng và hiệu quả. Công cụ này đặc biệt hữu ích trong việc kiểm tra, truy vết xử lý sự cố liên quan đến hệ thống DNS.

Hình 23: Bản đồ kiểm tra DNS bằng công cụ DNSChecker

2.2. DNSviz

- Địa chỉ: https://dnsviz.net
- DNSViz là một công cụ sử dụng để phân tích, kiểm tra, và trực quan hóa trạng thái của hệ thống DNS, đặc biệt là hỗ trợ đánh giá việc triển khai DNSSEC.



Hình 24: Kiểm tra DNSSEC bằng công cụ DNSviz

2.3. DNS Watch by VNNIC

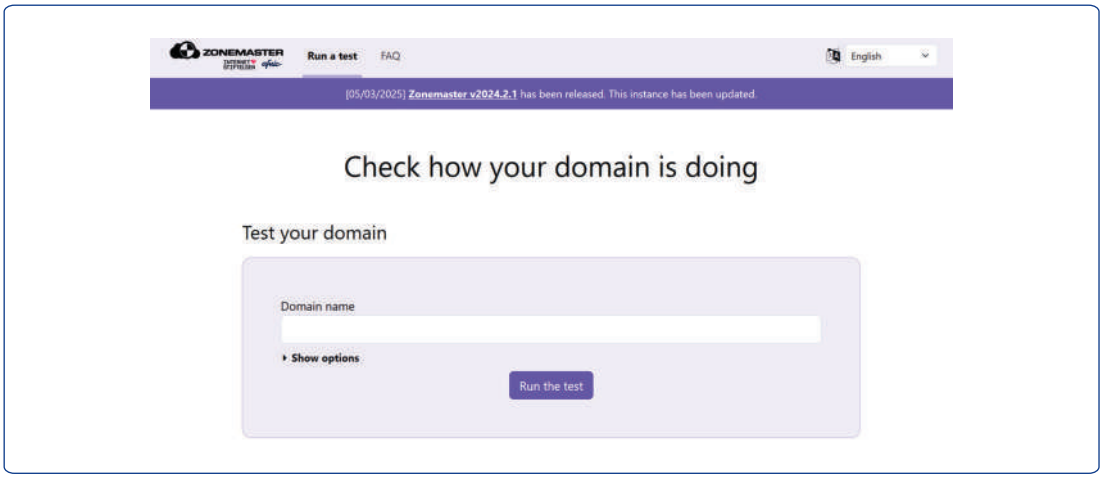
- Địa chỉ: https://internetatlas.vnnic.vn/dns-watch
- DNS Watch là một một công cụ giám sát, phân tích và trực quan hóa trạng thái vận hành của hệ thống DNS, bao gồm kiểm tra các thông số khai báo chi tiết của bản ghi SOA, kiểm tra tính đồng bộ hóa giữa các máy chủ DNS chuyển giao và thông tin khai báo bản ghi NS trên parent zone, ... đồng thời kiểm tra tính khả dụng của máy chủ DNS (kết nối qua cổng giao thức 53/TCP và 53/UDP trên cả IPv4 và IPv6).

Hình 25: Kiểm tra DNS bằng công cụ DNS Watch by VNNIC

2.4. Zonemaster.net:

- Địa chỉ: https://zonemaster.net/
- Zonemaster là công cụ kiểm tra toàn diện cấu hình DNS, phát triển bởi AFNIC (Pháp) và IIS (Thụy Điển). Bao gồm các chức năng chính:

+ Kiểm tra độ chính xác và tuân thủ RFC của cấu hình DNS.
+ Đánh giá khả năng chịu lỗi và độ ổn định của hệ thống DNS.
+ Hỗ trợ kiểm tra DNSSEC, IPv6, cấu hình SOA, NS, MX, TXT records.



Hình 26: Kiểm tra DNS bằng công cụ Zonemaster

3. Công cụ hỗ trợ điều tra, truy vết (Troubleshooting)

Việc chẩn đoán, điều tra, xử lý sự cố DNS có thể rất phức tạp, chủ yếu là do hệ thống DNS có sự tương tác với nhiều hệ thống tên miền khác. Một lỗi DNS có thể phát sinh từ một hoặc từ nhiều hệ thống máy chủ DNS trên mô hình tổng thể của DNS. Xác định vị trí chính xác của sự cố tùy thuộc vào cách tiếp cận của quản trị hệ thống, do đó trong quá trình chẩn đoán, điều tra và xử lý sự cố liên quan đến DNS cần có các công cụ hỗ trợ như sau:

3.1. Các công cụ hỗ trợ

Có rất nhiều công cụ hỗ trợ chẩn đoán DNS, đặc biệt là một số công cụ được thiết kế riêng cho hệ thống phần mềm BIND (đây là phần mềm DNS cơ bản và được sử dụng phổ biến cho các hệ thống DNS), trong khi những công cụ khác có thể chạy trên nhiều nền tảng khác nhau. Một số công cụ phổ biến được giới thiệu trong phần này bao gồm:

- **nslookup** – Công cụ truy vấn, có sẵn trên nhiều hệ điều hành, bao gồm Windows.
- **dig** – Tương tự với nslookup, đây là công cụ được sử dụng để truy vấnDNS, chủ yếu được sử dụng trên các hệ thống hỗ trợ BIND.
- **rndc** – Công cụ quản trị từ xa cho phần mềm BIND.
- **rndc-confgen** – Dùng để tạo khóa mã hóa và tệp cấu hình rndc.conf, giúp thiết lập quản lý máy chủ BIND một cách an toàn.
- **nsupdate** – Hỗ trợ cập nhật động các tệp dữ liệu zone DNS, đặc biệt hữu ích khi triển khai DHCP kết hợp với DNS động.
- **named-compilezone** – Công cụ giúp xác minh cấu trúc tệp dữ liệu zone DNS, đồng thời có thể chuyển đổi sang định dạng nhị phân để tăng tốc độ tải.
- **named-checkconf** – Kiểm tra cú pháp của tệp cấu hình named.conf, giúp phát hiện lỗi trước khi khởi động máy chủ DNS.
- **named-checkzone** – Kiểm tra độ chính xác của các tệp dữ liệu zone DNS để đảm bảo không có lỗi cấu hình.
- **dnssec-revoke** – Dùng để đặt cờ REVOKE trên các bản ghi DNSKEY, hỗ trợ trong quá trình quản lý khóa DNSSEC.
- **dnssec-settime** – Điều chỉnh tham số thời gian ký số DNSSEC.
- **dnssec-signzone:** Công cụ để ký số DNSSEC cho các zone tên miền.
- **dnssec-keygen**: Công cụ để tạo khóa mã hóa, đặc biệt thường được sử dụng trong DNSSEC.

Dưới đây là các phần mô tả và các ví dụ chi tiết về các công cụ hỗ trợ.

3.2. Công cụ nslookup

Ưu điểm lớn nhất của nslookup là tính khả dụng gần như phổ biến. Do đó, nếu làm việc trong môi trường hỗn hợp, chúng ta sẽ có nhiều khả năng sử dụng nslookup hơn là dig.

nslookup cung cấp cả hai chế độ: dòng lệnh (command line) và tương tác (interactive). Các tham số cấu hình của nslookup thường được cấu hình trong .nslookuprc của thư mục người dùng hoặc mặc định từ /etc/resolv.conf trên Linux, hoặc trong Network Properties trên Windows và có thể được sửa đổi trong chế độ interactive. Các tham số cấu hình mặc định có thể được hiển thị bằng cách sử dụng tùy chọn -all hoặc thiết lập tất cả tùy chọn trong chế độ tương tác với set all.

- Truy vấn sử dụng máy chủ mặc định
  nslookup [-opt] target
- Truy vấn sử dụng máy chủ chỉ định cụ thể
  nslookup [-opt] target dns
- Chế độ tương tác với máy chủ mặc định
  nslookup [-opt]
- Chế độ tương tác với một máy chủ chỉ định cụ thể
  nslookup [-opt] - dns

Lưu ý rằng định dạng thứ 4 không hoạt động trên phiên bản nslookup gốc của Windows mà chỉ hoạt động trên các phiên bản BIND cài đặt trên Windows.

Ví dụ về nslookup:

Ví dụ 1: Dùng chế độ dòng lệnh với máy chủ mặc định để tra cứu một tên miền

```
# nslookup www.vnnic.vn
Server: ns1.vnnic.vn
Address: 192.168.2.53

Name: www.vnnic.vn
Address: 192.168.2.80
```

Lệnh này trả về bản ghi A của www.vnnic.vn sử dụng máy chủ tên miền mặc định (ns1.vnnic.vn), được xác định trong Network Properties trên Windows hoặc trong tệp /etc/resolv.conf trên Linux và BSD.

Ví dụ 2: Dùng chế độ dòng lệnh với máy chủ mặc định để tra cứu bản ghi PTR (phân giải ngược IP)

```
# nslookup 192.168.2.80
Server: ns1.vnnic.vn
Address: 192.168.2.53
```

Lệnh này trả về bản ghi PTR cho 192.168.2.80 trong hệ thống phân cấp tên miền ngược IN-ADDR.ARPA.

Ví dụ 3: Dùng chế độ dòng lệnh với một máy chủ cụ thể để tra cứu một tên miền

```
# nslookup www.vnnic.vn 192.168.255.53
Server: ns1.vnnic.vn
Address: 192.168.255.53

Name: www.vnnic.vn
Address: 192.168.2.80
```

Lệnh này trả về bản ghi A của www.vnnic.vn bằng cách sử dụng máy chủ tên miền 192.168.255.53. Định dạng lệnh này cho phép sử dụng cả địa chỉ IP hoặc tên máy chủ cho máy chủ tên cụ thể.

b) Chế độ tương tác (interactive) của nslookup

Chế độ tương tác của nslookup (định dạng 3 và 4) cung cấp một dấu nhắc (>) cho phép nhập các lệnh chỉ thị tiếp theo. Để thoát chế độ này, sử dụng Ctrl+C (Windows và Linux, BSD nếu không có lệnh nào đang chạy), Ctrl+D (Linux và BSD) hoặc lệnh exit (Windows, Linux, BSD). Nếu đang chạy một truy vấn, Ctrl+C sẽ hủy lệnh đó, hoặc nếu không có lệnh nào, nó sẽ thoát khỏi nslookup.

```
# nslookup -all
> ls vnnic.vn
// Liệt kê tất cả các bản ghi trong tên miền (cần có hỗ trợ
AXFR)
> ls -T TXT vnnic.vn
// Liệt kê tất cả các bản ghi TXT trong tên miền
> set domain=example.vn
// Đặt tên miền mặc định cho các truy vấn tiếp theo
> mail
// Tìm bản ghi mail server
> exit
```

c) Tùy chọn của nslookup

nslookup cung cấp nhiều tùy chọn khác nhau, giúp điều chỉnh cách thức hoạt động của nó. Một số tùy chọn này chỉ có sẵn trong chế độ tương tác. Phiên bản Windows còn bổ sung một số lệnh đặc biệt. Một số tùy chọn có thể được chỉ định trực tiếp trên dòng lệnh.

Bảng sau đây trình bày một số lệnh tương tác phổ biến của nslookup:

TUỲ CHỌN	THAM SỐ	HỆ ĐIỀU HÀNH	CHẾ ĐỘ	MÔ TẢ
ls	[opt] domain	W, I	I	Liệt kê tất cả thông tin của tên miền. Sử dụng AXFR để đồng bộ zone tên miền. Nếu AXFR bị vô hiệu hóa, lệnh sẽ báo lỗi. Có thể dùng các lệnh > hoặc >> file để ghi kết quả vào tệp. Các tùy chọn hỗ trợ: -a (CNAME), -d (tất cả bản ghi), -h (HINFO), -s (dịch vụ), -t (kiểu bản ghi cụ thể, ví dụ -t A).
lserver server	Dns	A, I	I	Đặt máy chủ tên miền cho các lệnh sau đó. Có thể nhập tên hoặc địa chỉ IP.
root	root-dns	A, I	I	Đổi máy chủ gốc cho các truy vấn.

Trong bảng tùy chọn nslookup, các ký hiệu sau đây được sử dụng để chỉ định phạm vi hỗ trợ của từng tùy chọn:

- **Cột Hệ điều hành**

W = Chỉ hỗ trợ trên Windows.
A = Hỗ trợ trên Windows, Linux và BSD.
U = Chỉ hỗ trợ trên Linux và BSD.

- **Cột Chế độ hoạt động**

B = Hỗ trợ cả chế độ tương tác (interactive) và dòng lệnh (command-line).
I = Chỉ hỗ trợ trong chế độ tương tác (interactive only).
C = Chỉ hỗ trợ trong chế độ dòng lệnh (command-line only).

Các tùy chọn được định nghĩa trong dưới đây có thể được sử dụng trong chế độ tương tác nếu được đặt trước bằng từ khóa set, hoặc được sử dụng trong dòng lệnh nếu đặt trước bằng dấu - (dấu gạch ngang hoặc dấu trừ).

- Khi được sử dụng trên dòng lệnh, tùy chọn chỉ ảnh hưởng đến một lệnh duy nhất và không được lưu lại.
- Khi được sử dụng với set trong chế độ tương tác, tùy chọn đó sẽ tồn tại cho đến khi bị thay đổi bởi một lệnh tương tự khác.

Trong chế độ tương tác, lệnh set all sẽ hiển thị danh sách tất cả các thiết lập mặc định (tương đương với lệnh nslookup -all trên dòng lệnh). Trong nhiều trường hợp, cũng có sẵn dạng rút gọn của các tùy chọn để tiện sử dụng.

Bảng: Các tùy chọn nslookup

TUỲ CHỌN	THAM SỐ	HỆ ĐIỀU HÀNH	CHẾ ĐỘ	XỬ LÝ
all	[opt] domain	A	B	Hiển thị danh sách các giá trị mặc định được sử dụng bởi nslookup, bao gồm cả máy chủ tên miền
class=	lass	A	B	Cho phép thiết lập giá trị lớp cho tất cả các lệnh tiếp theo và có thể nhận các giá trị không phân biệt chữ hoa/thường như IN (Internet - mặc định), ANY, CH (CHAOS), và HS (HESIOD).
domain=	domain-name	A	B	Cho phép đặt một miền cơ sở cho tất cả các lần tìm kiếm tiếp theo khi sử dụng trong chế độ tương tác. Miền mặc định được định nghĩa trong /etc/resolv.conf đối với hệ thống Linux hoặc BSD và trong Network Properties đối với hệ thống Windows. Khi thiết lập domain=, bất kỳ danh sách tìm kiếm (srchlist) nào trước đó sẽ bị đặt lại.
[no]debug, [no]deb		A	I	Kiểm soát việc hiển thị thông tin gỡ lỗi; debug (viết tắt là deb) bật chế độ này, trong khi nodebug (hoặc nodeb) tắt nó. Mặc định là nodebug.
[no]d2		A	I	Bật hoặc tắt chế độ gỡ lỗi nâng cao; d2 bật, nod2 tắt. Mặc định là nod2.
[no]def-name, [no] def		A	I	Kiểm soát việc thêm một tên miền (domain hoặc srchlist) vào mục tiêu tìm kiếm nếu nó không kết thúc bằng dấu chấm (.), tức là nó không phải là FQDN (Tên miền đầy đủ). Xem thêm mục search để biết mô tả đầy đủ.
[no]ignoretc		A	I	Kiểm soát xem lỗi cắt gói có bị bỏ qua (ignoretc) hay sẽ dẫn đến lỗi (noignoretc, mặc định là noignoretc).
[no]msxfer		W	I	Kiểm soát việc sử dụng phương thức truyền tải nhanh MS. msxfer bật, nomsxfer (mặc định) tắt.
[no]recurse, [no]rec		A	B	Kiểm soát hành vi truy vấn đệ quy recurse (mặc định) bật đệ quy, norecurse tắt.
[no]vc		A	I	Kiểm soát việc sử dụng TCP (vc) hoặc UDP (novc). Mặc định là novc.
[no]search, [no]sea		A	I	Điều khiển cách giá trị srchlist được sử dụng. search và defname có liên quan đến nhau dựa trên ma trận được hiển thị trong Bảng 9-3 đối với các mục tiêu không phải là FQDN.

TUỲ CHỌN	THAM SỐ	HỆ ĐIỀU HÀNH	CHẾ ĐỘ	XỬ LÝ
port=	port-no.	A	B	Thay đổi cổng mặc định từ 53 sang cổng được chỉ định bởi port-no.
type=, querytype=	rr-type	A	B	Có thể nhận hầu hết các giá trị loại RR không phân biệt chữ hoa/thường, bao gồm các loại meta như ANY, IXFR, và AXFR. Giá trị mặc định là type=A. Khi sử dụng type=ANY với một miền gốc sẽ trả về bất kỳ RR nào với mục nhập nhãn trống; điều này bao gồm SOA, NS, và MX nếu truy vấn được hướng đến máy chủ ủy quyền cho miền đó.
retry=	number	A	B	Kiểm soát số lần thử lại trước khi từ bỏ. Mặc định là 4.
root=	dns	A	B	Kiểm soát máy chủ tên được sử dụng khi truy vấn máy chủ gốc. Mặc định thường là f.root-servers.net trên Linux và BSD, và a.root-servers.net trên Windows.
srchlist=	dom1/dom2	A	I	Cho phép thiết lập danh sách tìm kiếm (tối đa sáu tên được phép, phân tách bằng dấu /).

Chú thích:

- **Cột Hệ điều hành:**

W = Chỉ dành cho Windows.

A = Windows, Linux, BSD.

U = Linux, BSD.

- **Cột Chế độ:**

B = Hỗ trợ cả chế độ dòng lệnh và chế độ tương tác.

I = Chỉ hỗ trợ chế độ tương tác.

C = Chỉ hỗ trợ chế độ dòng lệnh.

Các tùy chọn được định nghĩa trong bảng trên có thể được sử dụng trong chế độ tương tác nếu đặt trước bằng từ khóa set, hoặc trên dòng lệnh nếu đặt trước bằng dấu - (dấu trừ hoặc dấu gạch ngang). Khi được sử dụng trên dòng lệnh, tùy chọn chỉ ảnh hưởng đến một lệnh duy nhất (không được lưu lại). Khi sử dụng set trong chế độ tương tác, tùy chọn sẽ tồn tại cho đến khi bị thay đổi bởi một lệnh tùy chọn tương tự khác.

Trong chế độ tương tác, lệnh set all sẽ liệt kê các cài đặt mặc định (lệnh tương đương trên dòng lệnh sẽ là nslookup -all). Trong nhiều trường hợp, một dạng viết tắt cũng được cung cấp.

Ảnh hưởng của các tùy chọn search và defname

Bảng dưới đây mô tả mối quan hệ giữa các tùy chọn *search* và *defname* khi được sử dụng với *srchlist*.

search	defname	KẾT QUẢ
search	defname	Thêm tên miền từ srchlist cho đến khi tìm thấy câu trả lời.
nosearch	defname	Thêm tên miền từ domain.
nosearch	nodefname	Phải là một FQDN (Fully Qualified Domain Name - Tên miền đầy đủ).
search	nodefname	Phải là một FQDN.

Trong mọi trường hợp, kết quả hợp lệ đầu tiên sẽ kết thúc lệnh. srchlist không thể được sử dụng để tra cứu nhiều mục tiêu cùng lúc. Nói chung, srchlist hữu ích nhất với các tên miền con (subdomains), nhưng cũng có thể được sử dụng với các tên miền khác nhau.

Ví dụ: Chế độ dòng lệnh

Sử dụng lệnh sau để lấy bản ghi mail (MX) của một tên miền:

```
# nslookup -type=MX vnnic.vn
```

Lệnh sau đây sẽ liệt kê tất cả các tùy chọn đang được sử dụng và lấy địa chỉ máy chủ cho mail.vnnic.vn:

```
# nslookup -all mail.vnnic.vn
```

Lệnh tiếp theo lấy bản ghi SOA (Start of Authority) bằng cách sử dụng một máy chủ DNS cụ thể:

```
# nslookup -type=SOA vnnic.vn 192.168.23.53
```

Lệnh truy vấn tất cả các bản ghi mà không có nhãn (label – thường là các bản ghi bao gồm SOA, NS, MX và các bản ghi khác nếu có). Nếu truy vấn đến máy chủ Authoritative DNS Server cho tên miền, nó sẽ trả về tất cả các bản ghi; nếu không, nó chỉ trả về các bản ghi NS:

```
# nslookup -type=any vnnic.vn ns1.vnnic.vn
```

Cuối cùng, lệnh sau lấy tất cả bản ghi của tên miền nếu việc đồng bộ zone tên miền (AXFR) không bị hạn chế. Nếu đồng bộ zone tên miền (AXFR) bị vô hiệu hóa, lệnh sẽ trả về lỗi **BAD ERROR VALUE.**

```
# nslookup -type=any vnnic.vn ns1.vnnic.vn
```

Ví dụ: Chế độ tương tác (Interactive Mode)

Chế độ tương tác cho phép người dùng nhập và liệt kê các tùy chọn mặc định của **nslookup.** (Các dòng bắt đầu bằng // được sử dụng như nhận xét để mô tả chức năng của dòng lệnh bên dưới. Chỉ các dòng bắt đầu bằng dấu nhắc # hoặc > mới cần nhập vào hệ thống)

```
# nslookup -all
Default Server: ns1.vnnic.vn
Address: 192.168.2.53
Set options:
nodebug
 defname
 search
 recurse
 nod2
 novc
 noignoretc
 port=53
 type=A
 class=IN
 timeout=2
 retry=1
 root=A.ROOT-SERVERS.NET.
 domain=vnnic.vn
 MSxfr [note: Windows only MS fast zone xfer]
 IXFRversion=1 [note: Windows only incremental zone xfer]
 srchlist=vnnic.vn

// Liệt kê tất cả bản ghi trong tên miền – cần bật axfr để hoạt động
> ls vnnic.vn
// Liệt kê tất cả các bản ghi TXT trong tên miền
> ls -t TXT vnnic.vn
// Đặt tên miền xác định được sử dụng cho các lệnh tiếp theo
> set domain=example.vn
// Tìm kiếm một máy chủ cụ thể
> mail
// Trả về mail.example.vn
// Sẽ xử lý cả định dạng đầy đủ
> mail.example.vn
// Trả về mail.example.vn như mong đợi
// Liệt kê các bản ghi của tên miền vnnic.vn
> set type=any
> vnnic.vn
// Ghi đè giá trị tên miền đã đặt trước đó
> set type=mx
```

```
// Lệnh này sẽ tồn tại trong suốt phiên làm việc
> vnnic.vn

// Chuyển đổi sang tìm kiếm bản ghi A để lấy địa chỉ IP
> set type=a
> www.vnnic.vn
// Hoạt động như mong đợi và trả về địa chỉ IP
// Chuyển đổi sang tìm kiếm tất cả bản ghi
> set type=any
> www.vnnic.vn
// Lệnh này sẽ trả về TẤT CẢ bản ghi có tên miền tương ứng
// Thoát khỏi chế độ tương tác
> exit
```

Tối ưu hóa truy vấn với nslookup

- Mặc định, nslookup sẽ tìm kiếm bản ghi loại A (chỉ trả về bản ghi A).
- Để có kết quả toàn diện hơn, nên thay đổi kiểu truy vấn sang ANY bằng cách sử dụng lệnh:

```
>set type=ANY
```

Điều này sẽ giúp chúng ta nhận về tất cả bản ghi DNS có liên quan đến tên miền, bao gồm cả bản ghi A, MX, TXT, NS, CNAME,... nếu có. Tùy chọn này giúp tối đa hóa thông tin thu được trong một lần truy vấn.

3.3. Công cụ BIND dig

Công cụ **dig (Domain Information Groper)** hiện là công cụ tra cứu, phân tích và chẩn đoán DNS được ưu tiên sử dụng. Tuy nhiên, như đã đề cập trước đó, nó không phải lúc nào cũng có sẵn, đặc biệt là trên hệ điều hành Windows. dig hoạt động ở cả hai chế độ: dòng lệnh và chế độ hàng loạt (batch mode), nhưng không hỗ trợ chế độ tương tác như nslookup.

Nhìn chung, cú pháp dòng lệnh của dig mạnh mẽ hơn nslookup, thậm chí còn cho phép thực hiện nhiều truy vấn trong một dòng lệnh duy nhất, trong khi chế độ dig hàng loạt giúp dễ dàng thực hiện kiểm tra các tập tin truy vấn. Công cụ này có một tập hợp các tùy chọn khá đa dạng và phức tạp, nhưng phần dưới đây sẽ giới thiệu một số ví dụ đơn giản để, sử dụng.

Ngoài ra, dig hỗ trợ tên miền đa ngữ (IDN - Internationalized Domain Names for Applications) nếu được biên dịch bằng tùy chọn --with-idn. Lưu ý rằng tùy chọn này không phải tiêu chuẩn trên hệ điều hành Ubuntu/Debian nhưng lại là một lựa chọn tùy chọn dành cho người dùng trên hệ điều hành FreeBSD.

Cú pháp lệnh dig:

```
dig [@dns] [-q] domain [[-c] q-class] [[-t] q-type] [+q-opt] [-arguments] [%comment]
```

Lưu ý:

- *Lệnh dig sử dụng kết hợp giữa các đối số theo vị trí (positional arguments) và các tùy chọn nhận diện bằng dấu -, -- hoặc +. Điều này giúp giữ cho các truy vấn đơn giản luôn rõ ràng.*
- *Trong một số trường hợp, cần phân biệt rõ giữa tùy chọn q-type và q-class, vì vậy khi sử dụng giá trị ANY, tốt nhất là chỉ định cả hai thông số -t và -c.*

Các tùy chọn của dig:

Bảng dưới đây liệt kê các tùy chọn phổ biến nhất có thể sử dụng với dig:

THAM SỐ	GIÁ TRỊ	MÔ TẢ
@dns	Tên hoặc địa chỉ IP	Định nghĩa tên hoặc địa chỉ IP của máy chủ DNS được sử dụng để truy vấn. Giá trị mặc định được xác định trong tệp /etc/resolv.conf trên Linux/BSD hoặc Windows Network Properties. Nếu có mặt, nó phải được đặt trước bởi ký tự @.
domain	Tên miền	Xác định tên miền cần truy vấn. Không giống như nslookup, nếu đây là một địa chỉ IP, phải sử dụng tùy chọn -x. Có thể luôn đặt trước -q để tránh nhầm lẫn, nhưng điều này hiếm khi cần thiết.
q-type	RR (Resource Record)	Xác định loại bản ghi tài nguyên cần truy vấn. Có thể nhận các giá trị như ANY, AXFR, MX, TXT, ... Nếu bỏ qua, mặc định sẽ là A. Ví dụ: # dig www.vnnic.vn txt # dig -t txt www.vnnic.vn Để lấy danh sách đầy đủ các bản ghi, có thể sử dụng AXFR (nếu được cho phép): Dig @ns1.vnnic.vn vnnic.vn axfr
q-class	IN, ANY, HESIOD, CHAOS	Xác định lớp truy vấn (Query Class). Giá trị mặc định là IN (Internet). Khi sử dụng ANY, cần đặt trước -c để đảm bảo giá trị đúng cho cả q-type và q-class. Ví dụ: # dig vnnic.vn any # dig -c any -t any vnnic.vn

THAM SỐ	GIÁ TRỊ	MÔ TẢ
q-opt	Query Options	Các tùy chọn truy vấn DNS, được đặt trước bằng dấu cộng (+) để kiểm soát cách truy vấn hoạt động. Nhiều giá trị có thể xuất hiện trong một lệnh duy nhất.
	bufsize=-bytes	Xác định số byte tối đa được quảng bá trong bản ghi EDNS0 OPT meta. Có thể đặt từ 0 đến 65535. Chỉ áp dụng khi sử dụng tùy chọn dnssec. Giá trị mặc định là 4096.
	domain =name	Thay thế tên miền mặc định được tìm thấy trong resolv.conf.
	edns=version	Xác định phiên bản EDNS sẽ được sử dụng trong truy vấn. Giá trị mặc định là edns=0. Sử dụng +noedns để đặt lại giá trị đã xác định về mặc định.
	ndots=num	Xác định số dấu chấm tối thiểu phải có trong một tên miền trước khi được sử dụng như một tên hợp lệ. Nếu tên miền có ít dấu chấm hơn giá trị này, tên miền mặc định từ resolv.conf sẽ được thêm vào trước khi thực hiện truy vấn. Giá trị mặc định là 1.
	[no]aaonly	Kiểm soát việc sử dụng truy vấn có thẩm quyền (Authoritative Query Only). Giá trị mặc định là noaaonly.
	[no]aaflag	Đồng nghĩa với [no]aaonly.
	[no]additional	Kiểm soát việc in phần ADDITIONAL SECTION trong phản hồi. Giá trị mặc định là additional.
	[no]adflag	Kiểm soát cờ AD trong truy vấn. Nếu adflag được bật, trình phân giải sẽ trả về cờ AD=1 nếu zone DNS đã được ký và xác thực đầy đủ. Giá trị mặc định là noadflag. Không áp dụng nếu truy vấn đến máy chủ Authoritative DNS Server.
	[no]all	Bật hoặc tắt tất cả các cờ kiểm soát trong kết quả hiển thị, như additional hoặc comments. Giá trị mặc định là all.
	[no]answer	Kiểm soát việc hiển thị phần ANSWER SECTION trong phản hồi. Giá trị mặc định là answer.
	[no] authority	Kiểm soát việc hiển thị phần AUTHORITY SECTION trong phản hồi. Giá trị mặc định là authority.
	[no] besteffort	Kiểm tra kết quả dig có hiển thị phản hồi bị lỗi định dạng hay không. Giá trị mặc định là nobesteffort.

THAM SỐ	GIÁ TRỊ	MÔ TẢ
	[no] comments	Kiểm soát việc hiển thị các nhận xét trong kết quả truy vấn. Giá trị mặc định là comments.
	[no]cdflag	Đặt bit CD (Checking Disabled), ngăn trình phân giải đệ quy thực hiện kiểm tra xác thực DNSSEC trên các zone tên miền đã ký. Cần sử dụng cùng với tùy chọn dnssec. Giá trị mặc định là nocdflag.
	[no]cl	Kiểm soát việc hiển thị thông tin lớp (class) của bản ghi DNS. Giá trị mặc định là cl.
	[no]cmd	Kiểm soát việc hiển thị các tham số hợp lệ của lệnh dig. Giá trị mặc định là cmd.
	[no] defname	Đồng nghĩa với [no]search.
	[no]dnssec	Kiểm soát việc đặt bit DNSSEC OK (DO) trong phần mở rộng OPT, từ đó yêu cầu trình phân giải cung cấp thông tin bảo mật về DNSSEC. Giá trị mặc định là nodnssec.
q-opt	Query Options	Các tùy chọn truy vấn DNS, được đặt trước bằng dấu cộng (+) để kiểm soát cách truy vấn hoạt động. Nhiều giá trị có thể xuất hiện trong một lệnh duy nhất.
	bufsize=-bytes	Xác định số byte tối đa được sử dụng trong bản ghi EDNS0 OPT meta. Có thể đặt từ 0 đến 65535. Chỉ áp dụng khi sử dụng tùy chọn dnssec. Giá trị mặc định là 4096.
	domain =name	Thay thế tên miền mặc định được tìm thấy trong resolv.conf.
	edns= version	Xác định phiên bản EDNS sẽ được sử dụng trong truy vấn. Giá trị mặc định là edns=0. Sử dụng +noedns để đặt lại giá trị đã xác định về mặc định.
	ndots=num	Xác định số dấu chấm tối thiểu phải có trong một tên miền trước khi được sử dụng như một tên miền hợp lệ. Nếu tên miền có ít dấu chấm hơn giá trị này, tên miền mặc định từ resolv.conf sẽ được thêm vào trước khi thực hiện truy vấn. Giá trị mặc định là 1.
	[no]aaonly	Kiểm soát việc sử dụng truy vấn Authoritative Query Only. Giá trị mặc định là noaaonly.
	[no]aaflag	Đồng nghĩa với [no]aaonly.
	[no] additional	Kiểm soát việc hiển thị phần ADDITIONAL SECTION trong phản hồi. Giá trị mặc định là additional.
	[no]adflag	Kiểm soát cờ AD trong truy vấn. Nếu adflag được bật, trình phân giải sẽ trả về cờ AD=1 nếu zone DNS đã được ký và xác thực đầy đủ. Giá trị mặc định là noadflag. Không áp dụng nếu truy vấn đến máy chủ Authoritative DNS Server.
	[no]all	Bật hoặc tắt tất cả các cờ kiểm soát trong kết quả hiển thị, như additional hoặc comments. Giá trị mặc định là all.
	[no]answer	Kiểm soát việc hiển thị phần ANSWER SECTION trong phản hồi. Giá trị mặc định là answer.
	[no]authority	Kiểm soát việc hiển thị phần AUTHORITY SECTION trong phản hồi. Giá trị mặc định là authority.
	[no] besteffort	Kiểm tra kết quả dig có hiển thị phản hồi bị lỗi định dạng hay không. Giá trị mặc định là nobesteffort.
	[no] comments	Kiểm soát việc hiển thị các nhận xét trong kết quả truy vấn. Giá trị mặc định là comments.

THAM SỐ	GIÁ TRỊ	MÔ TẢ
	[no]cdflag	Đặt bit CD (Checking Disabled), ngăn trình phân giải đệ quy thực hiện kiểm tra xác thực DNSSEC trên các zone tên miền đã ký. Cần sử dụng cùng với tùy chọn dnssec. Giá trị mặc định là nocdflag.
	[no]cl	Kiểm soát việc hiển thị thông tin lớp (class) của bản ghi DNS. Giá trị mặc định là cl.
	[no]cmd	Kiểm soát việc hiển thị các tham số hợp lệ của lệnh dig. Giá trị mặc định là cmd.
	[no] defname	Đồng nghĩa với [no]search.
	[no]dnssec	Kiểm soát việc đặt bit DNSSEC OK (DO) trong phần mở rộng OPT, từ đó yêu cầu trình phân giải cung cấp thông tin bảo mật về DNSSEC. Giá trị mặc định là nodnssec.
	[no]fail	Kiểm soát việc dig có dừng xử lý khi nhận được thông báo lỗi SERVFAIL từ một trong các máy chủ DNS mặc định được liệt kê trong resolv.conf hay không. Giá trị mặc định là fail.
	[no]identify	Chỉ hợp lệ với tùy chọn ngắn, kiểm soát việc ẩn hoặc hiển thị danh tính của máy chủ DNS. Giá trị mặc định là noidentify.
	[no]ignore	Kiểm soát việc bỏ qua các lỗi cắt bớt gói tin (truncation errors) thay vì thử lại bằng TCP. Giá trị mặc định là noignore, có nghĩa là dig sẽ tự động thử lại bằng TCP nếu gói tin bị cắt bớt.
	[no]multiline	Hiển thị các bản ghi DNS dài theo định dạng nhiều dòng trong dấu ngoặc đơn để dễ đọc hơn. Giá trị mặc định là nomultiline.
	[no]nsid	Gửi yêu cầu NSID request (OPCODE = 3) khi thực hiện truy vấn. Hữu ích khi gửi truy vấn đến các máy chủ Anycast. Giá trị mặc định là nonsid.
	[no] nssearch	Nếu được đặt, dig sẽ thực hiện lấy bản ghi SOA từ từng máy chủ Authoritative DNS Server của tên miền đang được truy vấn. Giá trị mặc định là nonssearch.
	[no]question	Kiểm soát việc hiển thị phần QUESTION SECTION trong phản hồi DNS. Giá trị mặc định là question.
	[no]qr	Kiểm soát việc hiển thị truy vấn DNS được gửi đi (outgoing query). Giá trị mặc định là noqr.
	[no]recurse	Kiểm soát hành vi truy vấn đệ quy (recursive query). Truy vấn đệ quy bị vô hiệu hóa mặc định khi sử dụng nssearch và trace. Giá trị mặc định là recurse.
	[no]search	Kiểm soát việc sử dụng bất kỳ miền nào từ domain hoặc danh sách tìm kiếm (search list) trong resolv.conf. Giá trị mặc định là nosearch.
	[no]short	Kiểm soát việc chỉ hiển thị câu trả lời (answer) cho truy vấn DNS. Ví dụ: trong truy vấn A, chỉ hiển thị địa chỉ IP. Giá trị mặc định là noshort.
	[no] showsearch	Kiểm soát việc hiển thị kết quả trung gian (search) hay không (noshowsearch). Giá trị mặc định là noshowsearch. Chỉ áp dụng nếu đang sử dụng tùy chọn +search.
	[no] sigchase	Kiểm soát việc theo dõi chuỗi chữ ký (chains of trust) đối với các vùng DNS đã ký (signed zones). Tùy chọn này không được bật theo mặc định và yêu cầu dig được biên dịch với DDIG_SIGCHASE (tiêu chuẩn trên các gói Ubuntu/Debian, tùy chọn trên FreeBSD). Giá trị mặc định là nosigchase.
	[no]stats	Kiểm soát việc hiển thị thống kê dig. Giá trị mặc định là stats.

THAM SỐ	GIÁ TRỊ	MÔ TẢ
	[no]tcp	Kiểm soát việc sử dụng TCP (tcp) hoặc UDP (notcp) cho truy vấn DNS. Giá trị mặc định là notcp, trừ khi sử dụng AXFR hoặc IXFR.
	[no] topdown	Kiểm soát việc xác thực chữ ký (signature validation) có được thực hiện theo kiểu từ trên xuống (top-down) hay không. Tùy chọn này không được bật theo mặc định và yêu cầu dig được biên dịch với DDIG_SIGCHASE (tiêu chuẩn trên các gói Ubuntu/Debian, tùy chọn trên FreeBSD). Giá trị mặc định là notopdown.
	[no]trace	Khi bật trace, dig sẽ hủy kích hoạt đệ quy (recursion), gửi truy vấn trực tiếp đến các máy chủ gốc (root-servers), theo dõi và hiển thị toàn bộ quá trình truy vấn cho đến khi tìm được máy chủ tên có thẩm quyền (authoritative name server). Giá trị mặc định là notrace.
	[no]ttlid	Kiểm soát việc hiển thị TTL (Time-To-Live). Giá trị mặc định là ttlid.
	[no]vc	Đồng nghĩa với [no]tcp.
	retry=num	Kiểm soát số lần thử lại (query retries) đối với mỗi máy chủ DNS. Giá trị mặc định là 2.
	time= seconds	Kiểm soát thời gian chờ (query timeout period) tính bằng giây. Giá trị mặc định là 4 giây.
	tries= number	Kiểm soát số lần thử (number of tries) đối với mỗi máy chủ DNS. Giá trị mặc định là 3.
	trusted -key=key	Xác định dữ liệu base64 để sử dụng làm khóa tin cậy (trusted key) khi kiểm tra chữ ký. Tùy chọn này không được bật theo mặc định và yêu cầu dig được biên dịch với DDIG_SIGCHASE (tiêu chuẩn trên Ubuntu/Debian, tùy chọn trên FreeBSD).
arguments	-4	Sử dụng IPv4. Chỉ hợp lệ đối với máy chủ hỗ trợ dual-stack (IPv4/IPv6).
	-6	Sử dụng IPv6. Chỉ hợp lệ đối với máy chủ hỗ trợ dual-stack (IPv4/IPv6).
	-b	Xác định địa chỉ IP được sử dụng trong truy vấn DNS (outgoing dig query). Chỉ yêu cầu khi sử dụng trên máy chủ có nhiều giao diện mạng (multihomed server).
	-c	Xác định rằng một đối số q-class sẽ theo sau (đây là định dạng tùy chọn được xác định) và có thể được sử dụng như một cách tiện lợi hoặc để phân biệt với cùng một loại tùy chọn q-type.
	-f filename	Chỉ định một tệp chứa các lệnh hàng loạt (batch commands). Bất kỳ tùy chọn nào được chỉ định trên dòng lệnh sẽ có hiệu lực trong suốt quá trình chạy hàng loạt, nghĩa là chúng có phạm vi toàn cục. Các dòng bắt đầu bằng ; hoặc # hoặc \n trong tệp hàng loạt sẽ bị bỏ qua và có thể được sử dụng làm chú thích hoặc dòng trắng. Mỗi dòng trong tệp hàng loạt sẽ đại diện cho một truy vấn dòng lệnh duy nhất.
	-k dir:key	Ký thông điệp bằng TSIG (Transaction Signature) bằng cách sử dụng tệp khóa nằm trong thư mục dir.
	-h	Hiển thị danh sách ngắn các tùy chọn của dig và thoát khỏi chương trình.
	-q	Chỉ định rằng đối số sau là một tên miền (domain argument).
	-p port	Thay đổi cổng được sử dụng cho các truy vấn (queries). Giá trị mặc định là 53.
	-t	Chỉ định rằng một đối số q-type (loại bản ghi DNS) sẽ theo sau (đây là định dạng đối số được xác định).
	-v	Hiển thị phiên bản của dig và thoát khỏi chương trình.

THAM SỐ	GIÁ TRỊ	MÔ TẢ
	-x	Chỉ định rằng sẽ sử dụng ký hiệu đảo ngược (inverse notation). Ví dụ: **Ví dụ sai (NXDOMAIN - không tìm thấy):** dig 192.168.2.53 **Ví dụ đúng:** dig -x 192.168.2.53 Hoặc nếu bạn muốn dùng cách thủ công: dig 53.2.168.192.in-addr.arpa ptr
	-y key	Cho phép người dùng nhập khóa chia sẻ base64 để sử dụng trong giao dịch TSIG. Tùy chọn này mất nhiều thời gian và có thể nguy hiểm. Chỉ sử dụng nếu bạn tuyệt vọng và tùy chọn -k không khả dụng.

Dưới đây là một lệnh tra cứu đơn giản cho một máy chủ (host lookup) mặc định trả về bản ghi A (A RR):

```
# dig www.vnnic.vn
```

Hoặc có thể được viết rõ ràng hơn với đối số sử dụng là bản ghi A

```
# dig www.vnnic.vn a
```

Lệnh này tương đương với lệnh trên nhưng sử dụng định dạng tùy chọn đã xác định (identified option format), do đó thứ tự không quan trọng:

```
# dig -t a www.vnnic.vn
```

Như đã đề cập trước đó, loại bản ghi (type) mặc định luôn là A. Sử dụng ANY sẽ giúp thu thập được nhiều kết quả hơn bằng cách trả về tất cả các loại bản ghi (RR types) tương ứng với tên miền nhất định.

Ví dụ:

- Trả về các bản ghi TXT, DKIM hoặc SPF nếu có (thường dành cho máy chủ email).
- Trả về bản ghi TXT, LOC hoặc thậm chí RP dành cho bản ghi A.
- Trả về cả bản ghi A và AAAA cho bất kỳ địa chỉ nào.

Ngoài ra, với sự phổ biến của DNSSEC, đây cũng là một cách đơn giản để kiểm tra xem dữ liệu (zone) có được ký xác thực (signed) hay không.

Ví dụ thực tế với dig:

Dưới đây là một ví dụ thực tế. Phần hiển thị chỉ bao gồm ANSWER SECTION trong đầu ra khi sử dụng hoặc không sử dụng ANY:

```
# dig www.vnnic.vn
;; ANSWER SECTION:
www.vnnic.vn. 84778 IN A 192.168.129.35
```

Khi sử dụng ANY để truy vấn tất cả các bản ghi:

```
# dig www.vnnic.vn any
;; ANSWER SECTION:
www.vnnic.vn.  84799 IN RRSIG A 5 3 86400 2011020210357 2011010310357 31662
vnnic.vn.      .jsj1AMH0xs1l1WLT1xiyvia1reegxhsby4bySduVih8PvBYEl9Izgrgfb      2pYtT2EHUKGydyJO-
JSevokw1LXA1v8hxlox18snuT/n9OMCpX1lWENr      12pnLNQ9Jr2ZDYG93V3ydLpx5J4ydLfyTxiU16mLiG/
q6VW6NrDgTqs1 KPU=
www.vnnic.vn.  84799 IN A 192.168.129.35
```

Sử dụng máy chủ tên miền cụ thể cho truy vấn:

Yêu cầu dig sử dụng máy chủ có địa chỉ IP 192.168.2.224 để thực hiện truy vấn:

```
# dig @192.168.2.224 www.vnnic.vn a
```

Yêu cầu dig sử dụng máy chủ DNS có hostname là ns1.vnnic.vn để thực hiện truy vấn:

```
# dig @ns1.vnnic.vn  www.vnnic.vn a
```

Truy vấn ngược bằng PTR:

Thực hiện một truy vấn ngược (reverse-map query) để trả về một bản ghi PTR:

```
# dig -x 192.168.2.224
```

Truy vấn nhiều tên miền bằng dig (dig Multiple Queries):

Lệnh dig cho phép truy vấn nhiều miền trong cùng một dòng lệnh - miễn là mỗi truy vấn được xác định rõ ràng (hoặc có sự phân biệt). Truy vấn dưới đây sẽ trả về các bản ghi tài nguyên không có nhãn (nonlabel RRs) cho cả hai miền:

```
# dig vnnic.vn any vnnic.net.vn any
```

Truy vấn dưới đây sẽ trả về bản ghi A cho miền đầu tiên và các bản ghi DNS (ANY) cho miền thứ hai:

```
# dig www.vnnic.vn vnnic.net.vn any
```

Nếu một dòng lệnh bắt đầu bằng một định dạng cụ thể, nó phải tuân thủ cùng định dạng đó. Lệnh dưới đây sẽ thất bại trên truy vấn tên miền thứ hai:

```
# dig vnnic.vn -t any vnnic.net.vn any
```

Tuy nhiên, định dạng này sẽ hoạt động cho cả hai tên miền:

```
# dig vnnic.vn -t any vnnic.net.vn -t any
```

Kết quả đầu ra của công cụ dig (dig Output):

Phần dưới đây hiển thị kết quả đầu ra từ một lệnh dig đơn giản truy vấn zone vnnic.vn bằng cách sử dụng một trong các máy chủ tên miền Authoritative DNS Server cho tên miền được truy vấn.

Lệnh sau được thực thi để truy vấn bản ghi A của www.vnnic.vn từ máy chủ tên miền ns1.vnnic.vn:

```
# dig @ns1.vnnic.vn www.vnnic.vn
```

Kết quả nhận được

```
;; <<>> DiG 9.3.0 <<>> @ns1.vnnic.vn www.vnnic.vn
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 826
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
www.vnnic.vn.  IN  A
;; ANSWER SECTION:
www.vnnic.vn.  86400  IN  A  10.1.2.1
www.vnnic.vn. 86400 IN A 192.168.254.3
www.vnnic.vn. 86400 IN A 172.16.2.1
www.vnnic.vn. 86400 IN A 192.168.2.5
;; AUTHORITY SECTION:
vnnic.vn. 86400 IN NS ns1.vnnic.vn.
vnnic.vn. 86400 IN NS ns2.vnnic.vn.
;; ADDITIONAL SECTION:
ns1.vnnic.vn. 86400 IN A 192.168.2.6
ns2.vnnic.vn. 86400 IN A 192.168.23.23
;; Query time: 31 msec
;; SERVER: 192.168.2.3#53(ns1.vnnic.vn)
;; WHEN: Tue May 31 20:16:25 2024
;; MSG SIZE rcvd: 165
```

Phân tích kết quả:

- *status: NOERROR → Truy vấn được xử lý thành công.*
- *QUERY: 1 → Một truy vấn đã được gửi.*
- *ANSWER: 4 → Nhận được 4 câu trả lời.*
- *AUTHORITY: 2 → Có 2 bản ghi trong phần Authority.*
- *ADDITIONAL: 2 → Có 2 bản ghi trong phần Additional.*

Cờ DNS (DNS Flags):

Các giá trị của các cờ (flags) trong phần >>HEADER<< của lệnh dig là kết quả của việc giải thích các bit khác nhau được thiết lập trong tiêu đề thông điệp (message header).

Các bit và ý nghĩa của chúng được mô tả chi tiết trong phần dưới đây:

- qr: Query Response (Phản hồi truy vấn), cờ này được thiết lập trong phản hồi của lệnh dig. Nó đơn giản chỉ ra rằng đây là phản hồi của một truy vấn và luôn được thiết lập trong phản hồi dig.
- aa: Authoritative Answer (Câu trả lời có thẩm quyền), cờ này được thiết lập trong phản hồi dig. Nó cho biết phản hồi đến từ một máy chủ Authoritative DNS Server đối với tên miền được truy vấn. Nếu truy vấn được gửi đến máy chủ Authoritative DNS Server lần đầu tiên, cờ này sẽ được đặt. Tuy nhiên, nếu phản hồi đến từ bộ nhớ đệm (cache), cờ này sẽ không bao giờ được thiết lập.
- rd: Recursion Desired (Yêu cầu đệ quy), cờ này được sao chép từ truy vấn (dig command) vào phản hồi. Nó có nghĩa là truy vấn ban đầu yêu cầu hỗ trợ đệ quy.
- ra: Recursion Available (Hỗ trợ truy vấn đệ quy), cờ này xuất hiện trong phản hồi dig và cho biết rằng máy chủ phản hồi (ví dụ: ns1.vnnic.vn) hỗ trợ truy vấn đệ quy.
- ad: Authenticated Data (Dữ liệu đã xác thực), cờ này không xuất hiện trong phản hồi dig trừ khi tùy chọn +dnssec được bật. Nó chỉ có hiệu lực với DNSSEC và chỉ ra rằng máy chủ đích có khả năng bảo mật DNSSEC (dnssec-enable yes trong tệp cấu hình named.conf). Nếu dữ liệu đến từ một zone tên miền đã ký (signed zone) và được xác thực hoàn toàn, cờ này sẽ được thiết lập.
- cd: Checking Disabled (Tắt kiểm tra DNSSEC), cờ này không xuất hiện trong phản hồi dig trừ khi tùy chọn +cdflag được bật. Nó chỉ có hiệu lực với DNSSEC và cho biết rằng truy vấn yêu cầu máy chủ DNS bỏ qua quá trình xác thực DNSSEC khi truy vấn một zone tên miền có ký DNSSEC (signed zone). Khi được thiết lập, máy chủ DNS sẽ không thực hiện kiểm tra chữ ký DNSSEC.
- do: DNSSEC OK (Chấp nhận DNSSEC), cờ này chỉ có hiệu lực với DNSSEC và xuất hiện trong phần OPT PSEUDOSECTION của phản hồi dig. Nó chỉ được thiết lập nếu tùy chọn +dnssec được bật và máy chủ đích hỗ trợ DNSSEC (dnssec-enable yes trong named.conf).

Trạng thái DNS (DNS Status) trong phản hồi dig:

Các giá trị trong trường trạng thái (status field) của phản hồi dig là một diễn giải của trường RCODE trong tiêu đề thông điệp, bản tin DNS. Dưới đây là các trạng thái phổ biến:

(1) Trạng thái thông thường:

- NOERR: Không có lỗi.
- FORMERR (Format Error): Lỗi định dạng - máy chủ DNS không thể hiểu được truy vấn.
- SERVFAIL (Server Failure): Lỗi máy chủ - máy chủ không thể xử lý truy vấn do sự cố nội bộ hoặc do một tính năng được yêu cầu không thể đáp ứng do vấn đề cấu hình.
- NXDOMAIN (Name Error): Lỗi tên miền - chỉ xuất hiện khi phản hồi đến từ một máy chủ Authoritative DNS Server, cho biết tên miền trong truy vấn không tồn tại.

(2) Trạng thái nâng cao:

- NOTIMP (Not Implemented): Không được triển khai - máy chủ DNS không hỗ trợ thao tác được yêu cầu (trước phiên bản BIND 9.3, mã phản hồi là NOTIMPL, tuy nhiên sau đó được chuẩn hóa thành NOTIMP).
- REFUSED: Máy chủ từ chối thực hiện thao tác theo chính sách bảo mật hoặc hạn chế truy cập. Ví dụ, máy chủ có thể không muốn cung cấp thông tin cho người yêu cầu hoặc từ chối thực hiện thao tác như đồng bộ zone tên miền (AXFR).
- YXDomain: Tên miền tồn tại trong khi khuyến nghị của RFC là không nên có (RFC 2136).
- YXRSet: Bộ bản ghi RR tồn tại trong khi khuyến nghị của RFC là không nên có (RFC 2136).
- NXRRSet: Bộ bản ghi RR cần tồn tại theo khuyến nghị của RFC nhưng thực tế không có (RFC 2136).
- NotAuth: Máy chủ không có thẩm quyền đối với zone tên miền được yêu cầu (RFC 2136).
- NotZone: Tên miền không thuộc zone tên miền đang truy vấn (RFC 2136).

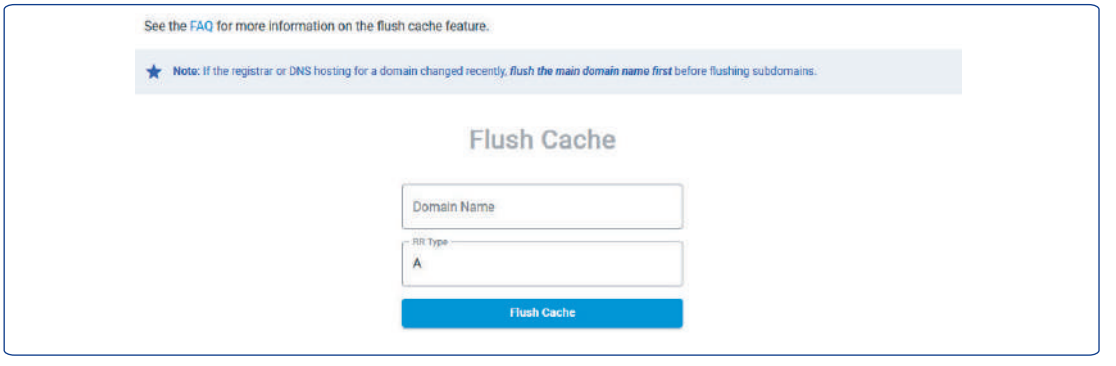
Ngoài ra các một số công cụ trực tuyến khác hỗ trợ chẩn đoán, xử lý sự cố như dnsviz.net, zonemaster.net, diggui.com, dnschecker.com, ... như đã giới thiệu ở phần trước.

3.4. Công cụ hỗ trợ xóa bộ nhớ đệm (Clear cache)

Trong một số trường hợp, một số tên miền cần thay đổi, cập nhật bản ghi DNS và yêu cầu thực hiện quảng bá cập nhật (propagation) một cách nhanh chóng là rất quan trọng, nhằm giảm thiểu thời gian ngưng trệ (down-time) của hệ thống. Tuy nhiên theo nguyên tắc hoạt động của hệ thống DNS, cụ thể là bộ nhớ đệm của các hệ thống DNS resolver (Public DNS, DNS của các ISP) sẽ lưu trữ thông tin với một thời gian TTL xác định. Để có thể thực hiện "flush" xóa bộ nhớ đệm trên các hệ thống Recursive DNS, chúng ta có các phương pháp thực hiện như sau:

- Xóa bộ nhớ đệm thông qua API của các tổ chức cung cấp dịch vụ Public DNS (như Google, Cloudflare,...).

+ Đối với DNS của Google: Truy cập vào giao diện API với đường dẫn và thực hiện theo hướng dẫn: https://developers.google.com/speed/public-dns/cache



Hình 27: Công cụ flush cache DNS của Google

Tại đây chúng ta sẽ nhập <Domain Name> là tên miền cần thực hiện xóa "flush" cache, và lựa chọn bản ghi phù hợp (RR Type).

+ Đối với DNS của Cloudflare: Tương tự với Google, Cloudflare cung cấp API cho phép thực hiện flush cache trên hệ thống Public DNS của Cloudflare (1.1.1.1) tại đường dẫn: https://one.one.one.one/purge-cache/

Sau khi truy cập vào đường dẫn trên sẽ xuất hiện giao diện như sau:

Hình 28: Công cụ flush cache của Cloudflare

Trong đó, <Domain Name> sẽ nhập tên miền cần thực hiện xóa cache, đồng thời lựa chọn bản ghi (Record Type) phù hợp tương ứng.

Sau khi thực hiện thao tác xóa bộ nhớ đệm ("flush" cache) thông qua các công cụ trên, thì ngay lập tức toàn bộ các máy chủ Public DNS của Google và Cloudflare sẽ xóa toàn bộ thông tin cache liên quan đến tên miền đang được cache trên chính các hệ thống đó.

Mục đích của việc này nhằm xóa thông tin "đã cũ" của tên miền trên các máy chủ Public DNS và khi có truy vấn, yêu cầu truy cập mới từ người dùng đến tên miền này, hệ thống sẽ truy vấn và lưu vào cache thông tin mới nhất.

+ Ngoài ra, nếu trên các hệ thống máy chủ Recursive DNS mà chưa hỗ trợ API hoặc trên các hệ thống Recursive DNS riêng của doanh nghiệp, tổ chức (sử dụng phần mềm BIND) thì có thể sử dụng công cụ "rndc" để xóa "flush" cache một cách nhanh chóng:

```
#rndc flush // flush toàn bộ bộ nhớ đệm (cache)
Hoặc:
#rndc flushname vnnic.vn //đối với tên miền cụ thể
```

4. Ghi nhật ký (Logging)

Logging hay ghi nhật ký log hệ thống là rất quan trọng đối với bất kỳ hệ thống thông tin nào và đối với hệ thống, phần mềm DNS cũng vậy. Việc ghi, quản lý nhật ký hệ thống đặc biệt quan trọng trong việc quản lý, vận hành và đặc biệt là điều tra, phân tích xử lý sự cố liên quan đến hệ thống DNS.

Trong nội dung phần này sẽ mô tả chi tiết các loại log (nhật ký) và cách tổ chức ghi nhật ký đối với hệ thống DNS sử dụng phần mềm BIND. BIND cung cấp, phân loại rất chi tiết và đầy đủ đối với các loại log (nhật ký) liên quan đến hoạt động của hệ thống DNS.

Cú pháp cấu hình logging có dạng như sau:

```
logging {
  [ channel channel_name {
    ( file path name
        [ versions ( number | unlimited ) ]
        [ size size_spec ]
      | syslog syslog_facility
      | stderr
      | null );
    [ severity (critical | error | warning | notice |
                info | debug [ level ] | dynamic ); ]
    [ print-category yes | no; ]
    [ print-severity yes | no; ]
    [ print-time yes | no; ]
  }; ]
  [ category category_name {
    channel_name ; [ channel_name ; ... ]
  }; ]
  ...
};
```

Trong đó, các tham số được giải thích chi tiết như sau:

- channel: BIND sẽ chấp nhận nhiều định nghĩa kênh (channel) trong một câu lệnh ghi nhật ký. 'channel_name' thường được viết dưới dạng một tên không có khoảng trắng, ví dụ như my_channel, nhưng nó cũng có thể được viết dưới dạng một chuỗi có dấu ngoặc kép, ví dụ như "my_channel". Đây là một tên tùy ý nhưng phải duy nhất, được sử dụng để liên kết câu lệnh phân loại với định nghĩa kênh này hoặc nó có thể nhận một trong các giá trị chuẩn (được định nghĩa sẵn) dưới đây:
+ "default_syslog": ghi tất cả vào syslog (tệp đích ghi nhật ký mặc định).
+ "default_debug": Ghi lại thông tin chi tiết về quá trình hoạt động của ứng dụng, bao gồm cả các thông báo gỡ lỗi.
+ "default_stderr": Ghi tất cả các thông tin nhật ký vào luồng lỗi chuẩn (stderr).
+ "null": loại bỏ tất cả các mục nhật ký (ghi vào /dev/null).
- file: 'path_name' là một chuỗi có dấu ngoặc kép định nghĩa đường dẫn tuyệt đối tới tệp nhật ký, ví dụ, "/var/log/named/namedlog.log".
- vesions: 'versions' có thể nhận tham số 'number' hoặc 'unlimited' và định nghĩa số lượng phiên bản tệp nhật ký mà BIND sẽ lưu lại. Các phiên bản tệp nhật ký được BIND tạo ra bằng cách thêm .0, .1, ... và tệp đã được định nghĩa trong tham số file.
- size: cho phép định nghĩa một giới hạn kích thước cho tệp nhật ký được tạo. Giá trị size_spec chỉ có số sẽ được coi là kích thước tính bằng byte, chúng ta có thể sử dụng các dạng rút gọn như k/K, m/M, g/G. size và versions có mối quan hệ như sau:
+ Nếu chỉ định giá trị size và KHÔNG chỉ định tham số versions, khi giới hạn kích thước được đạt đến giá trị đã chỉ định, BIND sẽ ngừng ghi nhật ký cho đến khi kích thước tệp giảm xuống dưới ngưỡng đã định, tức là bằng cách xóa hoặc cắt tệp.

+ Nếu chỉ định cả size và tham số versions, các tệp nhật ký sẽ được rotated (đổi tên và ghi đè như đã định nghĩa trong phần versions ở trên) khi đạt đến giới hạn kích thước quy định.
+ Nếu không chỉ định size và chỉ định tham số versions, các tệp nhật ký sẽ được rotated chỉ khi BIND được khởi động lại.

- syslog: chỉ ra rằng channel này sẽ sử dụng các tính năng ghi nhật ký của syslogd (như đã định nghĩa trong syslog.conf). syslog_facility là định nghĩa về facility cho 'syslog'. Theo cú pháp trên, 'file', 'syslog', 'stderr' và 'null' là không thể kết hợp với nhau trong một 'channel'.
- stderr: được ghi các nhật ký in/out theo chuẩn và thường chỉ được sử dụng cho các mục đích gỡ lỗi.
- null: ghi vào /dev/null - nơi không có dữ liệu, không tạo ra bất kỳ bản ghi nào.
- severity: định nghĩa các mức, cấp độ của log, nhật ký DNS sẽ được ghi lại: critical, errors, warning, notice, info, debug, dynamic.
- print-time: quy định ghi hoặc không ghi trường thời gian vào nhật ký (mặc định sẽ không nghi)
- print-severity: quy định mức độ nghiêm trọng có được ghi vào nhật ký hay không (mặc định là không)
- print-category: quy định mức độ nghiêm trọng có được ghi vào nhật ký hay không (mặc định là không).
- category: quy định các danh mục nào được ghi vào các 'channel_names' đã định nghĩa hoặc mặc định. category_name có thể nhận một trong các giá trị sau: client, config, database, default, delegation-only, dispatch, dnssec, general, lame-servers, network, notify, queries, resolver, rpz, rate-limit, security, unmatched, update, update-security, xfer-in, xfer-out. Trong đó, chỉ có các giá trị thường được sử dụng như:

+ Sử dụng cho máy chủ Authoritative DNS Server: queries, xfer-in, xfer-out, notify, update,...
+ Sử dụng cho máy chủ DNS Resolver: dnssec, security, rpz,...

Chi tiết các tệp cấu hình logging mẫu tham khảo tại: https://kb.isc.org/docs/aa-01526

PHẦN 2

BẢO MẬT VÀ ỨNG DỤNG CÔNG NGHỆ MỚI

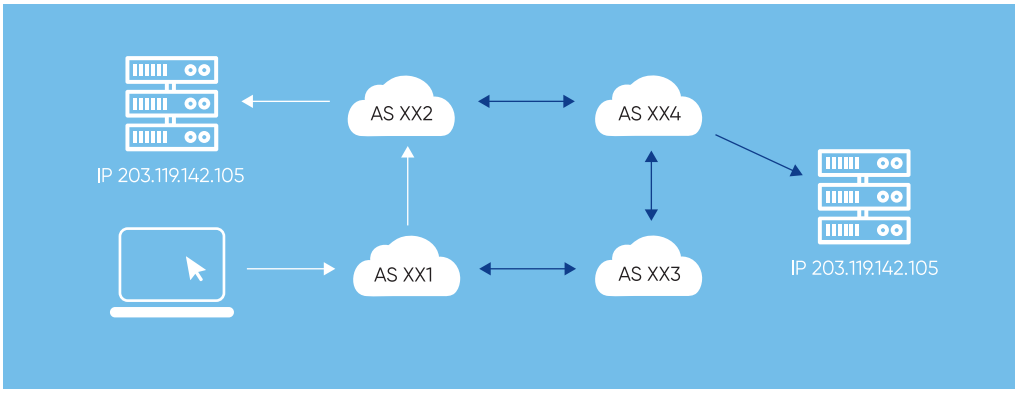
XI

GIẢI PHÁP DNS QUY MÔ LỚN, TĂNG CƯỜNG TÍNH SẴN SÀNG VÀ CHỐNG CHỊU

Trong bối cảnh ngày càng nhiều dịch vụ trực tuyến yêu cầu tính sẵn sàng cao và hiệu suất tối ưu, việc triển khai DNS quy mô lớn, có tính sẵn sàng và khả năng chống chịu cao trở nên rất quan trọng. Giải pháp công nghệ Anycast được sử dụng để triển khai hệ thống DNS trên diện rộng, đồng thời tăng cường tính sẵn sàng và khả năng chống chịu của hệ thống. Công nghệ Anycast cho phép định tuyến hiệu quả đến nhiều máy chủ, giảm thiểu độ trễ và cải thiện trải nghiệm người dùng. Nội dung dưới đây sẽ phân tích cụ thể giải pháp công nghệ này.

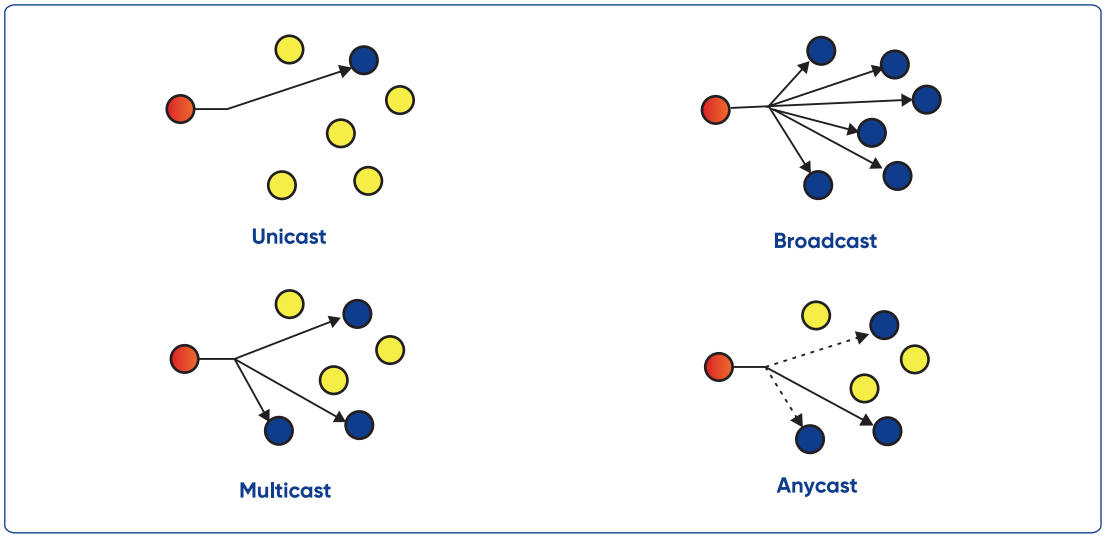
1. Anycast là gì

Anycast là kỹ thuật định tuyến trong đó một địa chỉ IP duy nhất được gán cho nhiều thiết bị (thường là máy chủ) đặt tại các vị trí khác nhau. Thay vì luôn hướng đến một máy đích cố định như unicast, lưu lượng gửi đến địa chỉ anycast sẽ được hệ thống định tuyến chuyển tới một trong những máy chủ có địa chỉ đó – cụ thể là máy chủ gần nhất theo các thông tin định tuyến (ví dụ: số chặng BGP ít nhất). Nói cách khác, anycast cho phép nhiều máy chủ chia sẻ cùng một IP và gói tin sẽ được định tuyến tới nút đích "gần" nhất, giúp tối ưu hóa đường đi.



Hình 29: Kỹ thuật định tuyến Anycast

So sánh Anycast với Unicast, Multicast, Broadcast:



Hình 30: So sánh Anycast, Unicast, Multicast và Broadcast

- **Anycast** khác biệt ở điểm đây là mô hình "một-ngưỡng-nhiều nhưng chỉ đến một đích duy nhất", nghĩa là gói tin có thể có nhiều máy chủ đích nhưng chỉ một máy chủ gần nhất thực sự nhận gói tin.
- **Unicast** là "một-một", nghĩa là một địa chỉ IP duy nhất đại diện cho một máy nhận duy nhất, mọi dữ liệu gửi đến địa chỉ đó đều đến cùng một máy (tương tự như địa chỉ nhà cụ thể).
- **Broadcast** là "một-tất cả", nghĩa là một nút gửi dữ liệu đến tất cả các nút trong cùng một mạng (ví dụ địa chỉ broadcast trong LAN sẽ phát gói tin đến mọi thiết bị trong mạng đó).
- **Multicast** là "một-nhiều (nhóm)" hoặc "nhiều-nhiều", nghĩa là gói tin được gửi tới một nhóm các máy quan tâm, sử dụng một địa chỉ nhóm chung. Các bộ định tuyến sẽ nhân bản gói tin và phân phát cho nhiều máy nhận thuộc nhóm đó, thay vì cho tất cả.

Khái niệm anycast đã xuất hiện từ cuối những năm 1980. Năm 1989, phương pháp định tuyến anycast bắt đầu được sử dụng thử nghiệm để cân bằng tải theo các mô hình mạng cho các dịch vụ Internet. Đến năm 1993, nguyên lý này được chuẩn hóa chính thức trong RFC 1546 của IETF với tên gọi "Host Anycasting Service", đề xuất việc dùng địa chỉ anycast chia sẻ giữa các máy chủ để tăng hiệu năng mạng và hỗ trợ tự cấu hình cho DNS Resolver. Tuy nhiên, vào thập niên 1990, việc triển khai anycast còn hạn chế do không phải thiết bị nào cũng hỗ trợ nhận gói tin gửi đến địa chỉ anycast và cũng tồn tại lo ngại về an toàn an ninh. Đến cuối những năm 1990, IETF tiếp tục mở rộng anycast cho IPv6 (RFC 2526 năm 1999).

Việc ứng dụng anycast thực sự tăng mạnh trong lĩnh vực DNS vào đầu những năm 2000. Năm 2001, máy chủ I-Root (DNS Root) là hạ tầng quan trọng đầu tiên áp dụng anycast. Từ khoảng năm 2003–2006, nhiều cụm máy chủ DNS Root đã bắt đầu triển khai anycast nhằm nâng cao chất lượng, cải thiện khả năng chịu tải, chống tấn công từ chối dịch vụ.

Đến cuối thập niên 2010, hầu hết các nhà cung cấp dịch vụ DNS lớn đều đã chuyển sang mô hình anycast để tăng tốc độ truy vấn, tăng tính dự phòng và cân bằng tải. Hiện nay, toàn bộ 13 cụm máy chủ DNS Root (A–M) của Internet đều triển khai ứng dụng anycast, mỗi cụm gồm nhiều máy chủ (instance) phân bố khắp toàn cầu.

Hình 31: Bản đồ các máy chủ DNS Root toàn cầu

2. Mối liên hệ giữa Anycast và DNS

- **Công nghệ Anycast quan trọng đối với DNS:** DNS được xem như là "danh bạ", hay là "sổ địa chỉ" của Internet, đóng vai trò phân giải tên miền sang địa chỉ IP và ngược lại. Tốc độ và độ tin cậy của DNS ảnh hưởng trực tiếp đến trải nghiệm người dùng Internet. Anycast được ứng dụng phù hợp với DNS vì hai lý do chính:
+ Hiệu năng – giúp giảm độ trễ truy vấn bằng cách trả lời từ máy chủ gần nhất.
+ Khả năng chịu lỗi – nhiều instance phân tán đảm bảo tính dự phòng tự động trong trường hợp một hoặc vài máy chủ gặp sự cố.

Nhiều nhà cung cấp DNS thương mại đã chuyển sang ứng dụng Anycast chính là để tăng tốc độ xử lý truy vấn và nâng cao tính dự phòng, đồng thời thực hiện cân bằng tải hiệu quả hơn giữa các máy chủ. Đối với hệ thống DNS toàn cầu, Anycast mang lại một tầng kiến trúc bổ sung bên cạnh các cơ chế dự phòng sẵn có của DNS (như nhiều bản ghi NS, Round-Robin), giúp hệ thống DNS hoạt động tối ưu hơn.

- **Tối ưu hóa tốc độ phân giải tên miền:** Anycast rút ngắn quãng đường giữa người dùng và máy chủ DNS, qua đó giảm thời gian phản hồi truy vấn. Thay vì mọi truy vấn phải đi đến một máy chủ cố định (có thể ở cách xa).
- **Bảo mật DNS với Anycast – Giảm thiểu tấn công DDoS:** Một lợi ích nổi bật khiến Anycast được ưu tiên và sử dụng phổ biến cho hệ thống DNS là khả năng chống chịu tấn công từ chối dịch vụ phân tán (DDoS). Với mô hình unicast truyền thống, kẻ tấn công chỉ cần dồn lưu lượng vào một địa chỉ IP máy chủ DNS là có thể làm quá tải dịch vụ. Nhưng trong kiến trúc Anycast, cùng một địa chỉ IP đó được "chia" cho nhiều máy chủ trên khắp thế giới. Khi xảy ra tấn công, lưu lượng tấn công sẽ được phân tán ra toàn mạng lưới thay vì dồn vào một điểm, nhờ đó giảm tải cho các máy chủ.

3. Công nghệ và nguyên tắc hoạt động của DNS Anycast

Sử dụng BGP để định tuyến Anycast: Trên phạm vi Internet toàn cầu, anycast thường được thực hiện thông qua giao thức định tuyến Border Gateway Protocol (BGP). Mỗi điểm hiện diện (Point of Presence – PoP) trong mạng anycast sẽ quảng bá cùng một tiền tố mạng (prefix) IP ra BGP.

Công nghệ Anycast cho phép triển khai nhiều máy chủ tại nhiều địa điểm khác nhau nhưng chỉ sử dụng 01 địa chỉ IP và tên miền duy nhất, điều đó đảm bảo việc tăng tốc độ trả lời truy vấn tên miền, chịu tải rất lớn và khả năng mở rộng, an toàn cao, hoàn toàn trong suốt với người sử dụng.

Ví dụ, một dịch vụ DNS Anycast có thể dùng địa chỉ IPv4/24 hoặc IPv6/48 chung cho tất cả các máy chủ. Mỗi máy chủ sẽ thiết lập phiên BGP (thường là eBGP) với nhà cung cấp transit hoặc tại điểm trao đổi Internet (IX) để quảng bá prefix Anycast. Kết quả là bảng định tuyến trên Internet sẽ có nhiều tuyến đường cùng dẫn đến prefix Anycast đã được quảng bá, tương ứng với các địa điểm đặt máy chủ khác nhau. Dựa trên nguyên tắc hoạt động của BGP để lựa chọn tuyến đường tối ưu (thường ưu tiên tuyến đường có "path" ngắn nhất) để quyết định gửi lưu lượng tới các máy chủ DNS.

Xử lý truy vấn DNS trong hệ thống Anycast: Về bản chất, quá trình phân giải tên miền với DNS Anycast không khác biệt về mặt logic so với DNS thông thường, ngoài bước định tuyến đến máy chủ như đã trình bày ở trên.

Với kỹ thuật định tuyến Anycast, nếu cụm máy chủ gần nhất bị quá tải hoặc ngừng hoạt động, nó sẽ ngừng quảng bá định tuyến BGP; khi đó, gói tin DNS truy vấn gửi đến của người dùng sẽ tự động được định tuyến sang cụm anycast kế tiếp (ví dụ cụm gần thứ hai) mà không cần bất kỳ sự can thiệp nào từ phía người dùng, người quản trị, quá trình này diễn ra tự động ở lớp định tuyến. Do đó đảm bảo truy vấn DNS vẫn nhận được phản hồi từ phía máy chủ DNS.

4. Các mô hình triển khai DNS Anycast

DNS Anycast có thể được triển khai theo nhiều mô hình tùy theo đối tượng sử dụng và quy mô hạ tầng, từ dịch vụ DNS công cộng cho tới các mạng DNS riêng của doanh nghiệp tự quản lý. Dưới đây là một số mô hình tiêu biểu và hướng dẫn triển khai:

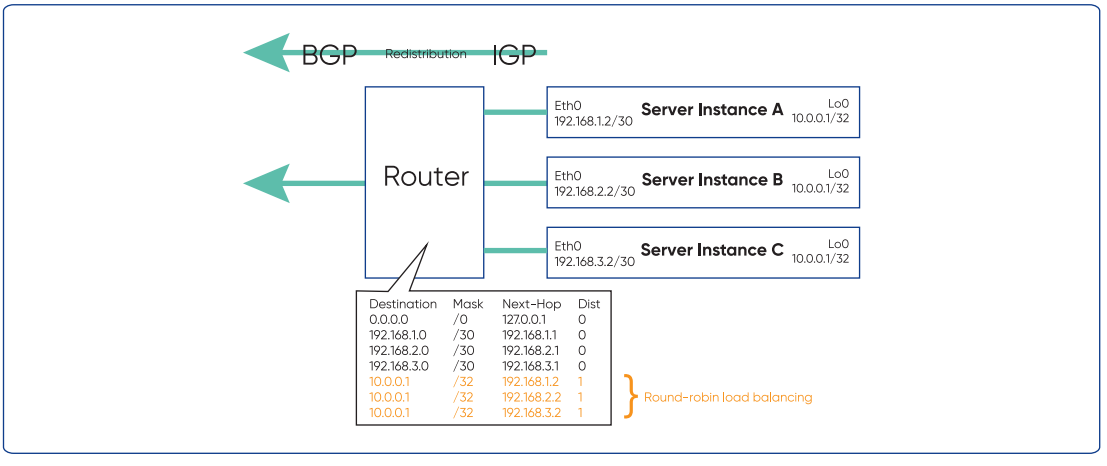
4.1. Mô hình local cluster

Mô hình này sẽ thực hiện triển khai tại 01 điểm gồm nhiều node (>=2 node). Các máy chủ kết nối vào hệ thống bằng địa chỉ kết nối, đồng thời cũng là địa chỉ quản lý.

Sử dụng giao diện ảo (sub-interface loopback) để làm giao diện chạy dịch vụ DNS.

Trên các node cài phần mềm DNS, cấu hình trả lời truy vấn trên địa chỉ anycast.

Router sẽ chuyển lưu lượng truy vấn DNS đến máy chủ DNS theo bảng định tuyến trên Router.



Hình 32: Mô hình local cluster trong Anycast

Mô hình này chỉ giải quyết vấn đề khả năng an toàn, dự phòng và tính sẵn sàng của dịch vụ tại một điểm, công nghệ áp dụng tương tự như công nghệ cân bằng tải CSM.

Để thực hiện chuyển gói tin đến các máy chủ, cách đơn giản nhất là cấu hình static route trên router đến các máy chủ tương ứng, router sẽ thực hiện round robin lần lượt đến các máy chủ. Cách làm này có ưu điểm là đơn giản nhưng có nhược điểm là khi có một máy chủ hoặc phần mềm DNS bị sự cố thì router không nhận biết được và vẫn chuyển gói tin đến máy chủ đó, điều này làm giảm chất lượng dịch vụ DNS.

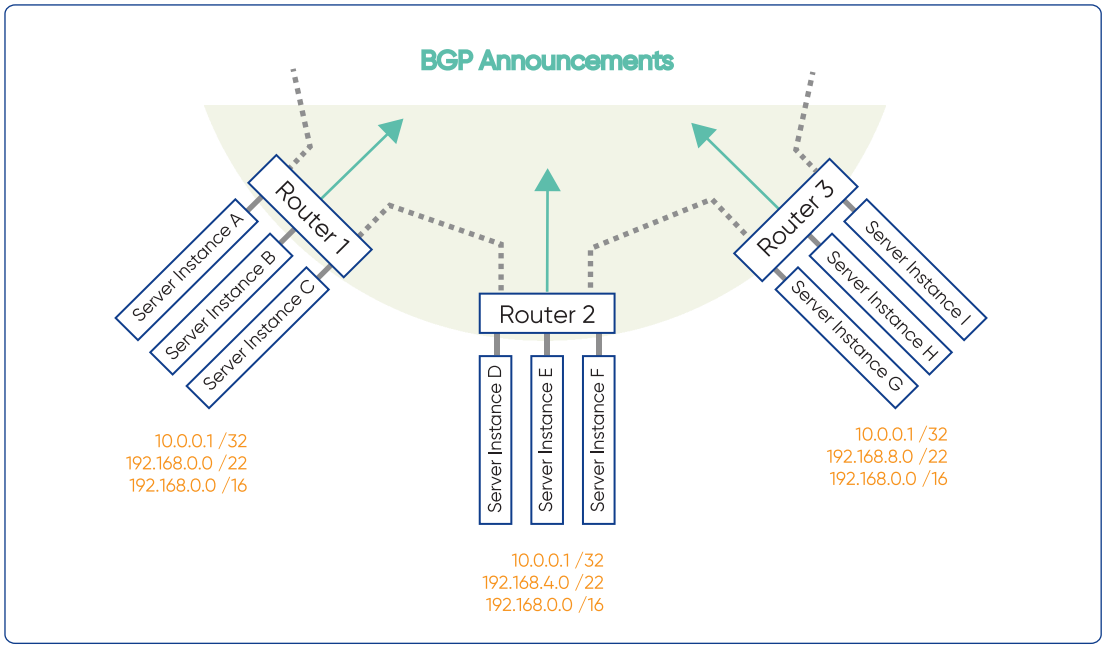
Để khắc phục nhược điểm này thì có thể sử dụng giải pháp định tuyến động giữa Router và máy chủ DNS để có thể tự động nhận biết tình trạng dịch vụ và cập nhật bảng định tuyến trên router liên tục theo tình trạng dịch vụ/máy chủ.

- Máy chủ gồm 02 địa chỉ: kết nối mạng thông thường để quản lý và địa chỉ Anycast dùng chung cho dịch vụ. Địa chỉ dịch vụ thường được gán vào giao diện loopback của máy chủ.
- Cài đặt phần mềm định tuyến trên máy chủ: có nhiều phần mềm opensource (Quagga, BIRD, ...)
- Thực hiện peering với Router, khi máy chủ có sự cố thì router sẽ tự động xóa bỏ định tuyến tới máy chủ tương ứng, toàn bộ lưu lượng sẽ được chuyển sang các máy chủ còn lại.

4.2. Mô hình global cluster:

Sau khi triển khai local cluster xong thì bước tiếp theo là triển khai mở rộng cụm máy chủ đó trên nhiều địa điểm nhằm đảm bảo an toàn, sẵn sàng cao:

- Sử dụng BGP Unicast Routing.
- Quảng bá số hiệu mạng và vùng địa chỉ sử dụng làm anycast tại nhiều địa điểm khác nhau tới ISP upstream.
- Tối ưu hóa định tuyến, chính sách định tuyến.



Hình 33: Mô hình global cluster trong Anycast

Lúc này cụm DNS anycast đã được triển khai theo mô hình đầy đủ, việc trả lời truy vấn vẫn qua địa chỉ Anycast, việc đồng bộ, quản trị qua địa chỉ quản lý, kết nối với ISP upstream.

5. Xu hướng phát triển DNS Anycast

Trong tương lai, DNS Anycast dự kiến sẽ tiếp tục mở rộng và đóng vai trò then chốt trong việc đảm bảo Internet hoạt động liên tục, an toàn và tin cậy. Một số xu hướng và yếu tố phát triển:

- Phổ cập trên nền IPv6: Khi IPv6 dần trở nên phổ biến, thì Anycast càng được sử dụng rộng rãi hơn. Không gian địa chỉ rộng lớn của IPv6 cho phép dễ dàng cấp các prefix /48 cho dịch vụ Anycast mà không lo thiếu/cạn kiệt địa chỉ.
- Mở rộng quy mô và hiệu năng: Nhu cầu phân giải tên miền sẽ tiếp tục tăng khi số lượng thiết bị IoT, người dùng Internet, dịch vụ trực tuyến ngày càng nhiều. DNS Anycast sẽ phải mở rộng thêm cả về quy mô mạng lưới lẫn công suất xử lý. Xu hướng chung là năng lực chịu tải của các hệ thống DNS Anycast sẽ ngày càng cao. Cùng với đó, các thuật toán cân bằng tải, cơ chế định tuyến anycast động, ... có thể được áp dụng để tối ưu hiệu suất.
- Anycast kết hợp điện toán biên và IoT: Sự phát triển của điện toán biên (edge computing) và IoT sẽ làm gia tăng nhu cầu phát triển mạng Anycast. Khi ngày càng nhiều dịch vụ được đưa ra biên (edge), việc có các điểm DNS gần biên là cần thiết. DNS Anycast có thể trở thành một phần của hạ tầng edge cloud, trong đó mỗi edge location có một node DNS Anycast phục vụ cả mục đích phân giải truyền thống lẫn dịch vụ đặc thù. Điều này giúp các thiết bị IoT hoặc ứng dụng edge giảm phụ thuộc vào trung tâm. Bên cạnh đó, Anycast có thể kết hợp với cơ chế multicast DNS (mDNS) trong IoT để tạo hệ thống phân giải đa tầng hiệu quả hơn.

DNS Anycast có giá trị ứng dụng to lớn trong việc nâng cao hiệu năng và độ ổn định của hệ thống phân giải tên miền (DNS). Dù vẫn còn những thách thức về quản lý và kỹ thuật, xu hướng và sự phát triển công nghệ cho thấy Anycast sẽ ngày càng an toàn hơn, thông minh hơn và được sử dụng rộng rãi hơn. Kết hợp với các biện pháp bảo mật như DNSSEC, RPKI và nhiều đặc điểm hỗ trợ trong cấu trúc địa chỉ IPv6, DNS Anycast sẽ tiếp tục là nền tảng vững chắc để Internet phục vụ hàng tỷ người dùng và thiết bị trong tương lai một cách nhanh chóng và tin cậy.

XII

BẢO MẬT DNS

1. Các mối đe doạ đối với DNS

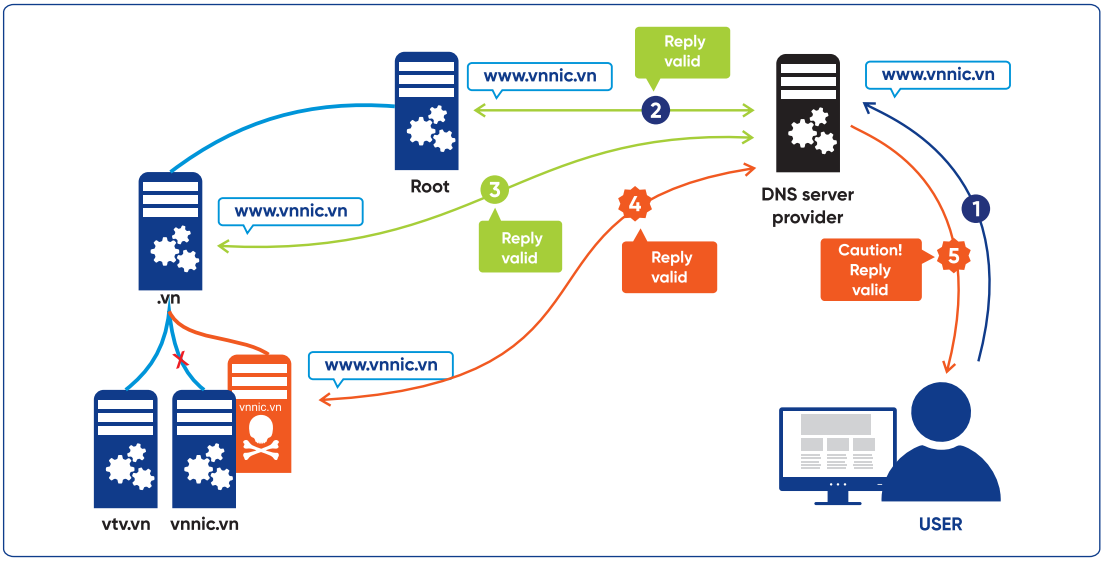
Hệ thống DNS là một hệ thống thông tin quan trọng trên Internet, do tính chất quan trọng đó của hệ thống DNS nên có rất nhiều kẻ tấn công và sử dụng các phương thức tấn công đa dạng, nhằm làm ngưng trệ hoạt động của hệ thống này hay đánh cắp, giả mạo các thông tin, ảnh hưởng rất lớn đối với các dịch vụ khác trên Internet và người dùng.

2. Một số dạng tấn công DNS phổ biến

2.1. Tấn công đầu độc bộ nhớ đệm (DNS Cache Poisoning)

Đây là một phương pháp tấn công DNS, thay đổi thông tin, giả mạo địa chỉ IP, tên miền tương ứng trên bộ nhớ đệm (cache) của máy chủ DNS và gửi các phản hồi giả mạo, chuyển hướng luồng truy cập đến một máy chủ độc hại cho người dùng.

Để khai thác theo hướng này, kẻ tấn công (attacker) lợi dụng lỗ hổng của phần mềm DNS, do các phản hồi truy vấn DNS không được xác thực để đảm bảo chúng được gửi từ các máy chủ DNS được xác thực, các bản ghi giả mạo sẽ được lưu lại trên bộ nhớ đệm của máy chủ DNS và phục vụ cho các người dùng khác.



Hình 34: Tấn công DNS Cache Poisoning

Bộ nhớ đệm DNS cache được tạo trên máy tính hoặc máy chủ DNS phân giải như DNS của các ISP nhằm giảm thời gian truy vấn DNS. Về cơ bản, DNS cache là một bộ nhớ tạm, chứa các thông tin liên quan đến tên miền, bản ghi và các địa chỉ IP được ánh xạ mà nó lưu lại được sau các hoạt động truy vấn, phản hồi truy vấn DNS trên nó và việc lưu tạm nhằm mục đích sử dụng cho lần truy vấn tương tự tiếp theo, cải thiện tốc độc phản hồi truy vấn DNS. Nếu trong bộ nhớ đệm có câu trả lời, máy chủ phân giải sẽ sử dụng nó. Nếu không máy chủ sẽ liên lạc với máy chủ DNS và tìm nạp câu trả lời. Sau đó, nó sẽ cập nhật bộ nhớ DNS cache cục bộ với thông tin mới nhất mà nó đã thực hiện được.

Mỗi thông tin bản ghi, tên miền hay địa chỉ IP trong bộ nhớ DNS cache đều có giới hạn thời gian, tùy thuộc vào hệ điều hành và chính sách của máy chủ phân giải DNS. Sau khi hết thời gian lưu tạm, máy chủ chứa DNS cache sẽ liên hệ với máy chủ DNS và cập nhật các thông tin sao cho chính xác.

Tuy nhiên, có những kẻ xấu muốn làm nhiễm độc bộ nhớ đệm cho mục đích xấu. Làm nhiễm độc bộ nhớ đệm có nghĩa là thay đổi giá trị thực của URL. Ví dụ, tội phạm mạng có thể tạo một trang web trông giống như xyz.com và nhập bản ghi DNS của nó vào DNS cache. Do đó, khi gõ xyz.com vào thanh địa chỉ của trình duyệt, trình duyệt thứ hai sẽ nhận địa chỉ IP của trang web giả mạo và đưa người dùng đến đó, thay vì trang web thực. Điều này được gọi là Pharming. Sử dụng phương pháp này, tội phạm mạng có thể phát hiện các thông tin xác thực đăng nhập của người dùng và nhiều thông tin khác như chi tiết thẻ, số an sinh xã hội, số điện thoại,... để ăn cắp dữ liệu

cá nhân. Việc làm nhiễm độc DNS cache cũng được thực hiện để đưa phần mềm độc hại vào máy tính hoặc mạng của người dùng. Khi người dùng truy cập trang web giả mạo bằng bộ nhớ DNS cache bị nhiễm độc, kẻ tấn công có thể làm bất cứ điều gì chúng muốn.

- **Một số kỹ thuật tấn công đầu độc bộ nhớ đệm:**

+ **Cách thứ 1: thiết lập một DNS Server giả mạo với các bản ghi độc hại.**

Mục đích là để lái các client khi phân giải một tên miền nào đó về địa chỉ IP giả mạo, ví dụ khi client cần phân giải địa chỉ www.cnn.com thì được trả về địa chỉ IP giả là 66.66.66.66. Khi nào bản ghi tên miền giả còn tồn tại trong cache của DNS Server nạn nhân, các truy vấn của www.cnn.com sẽ được chuyển hướng đến 66.66.66.66, đây có thể là một máy tính được đặt dưới sự kiểm soát của kẻ tấn công, các thông tin đến www.cnn.com sẽ được kẻ tấn công chuyển hướng đến nguồn độc hại, giả mạo. Do đó client cuối cùng không biết có sự tồn tại của máy "man in the middle".

+ **Cách thứ 2: Gửi một phản hồi giả mạo đến client thông qua việc thu thập, nghe lén.**

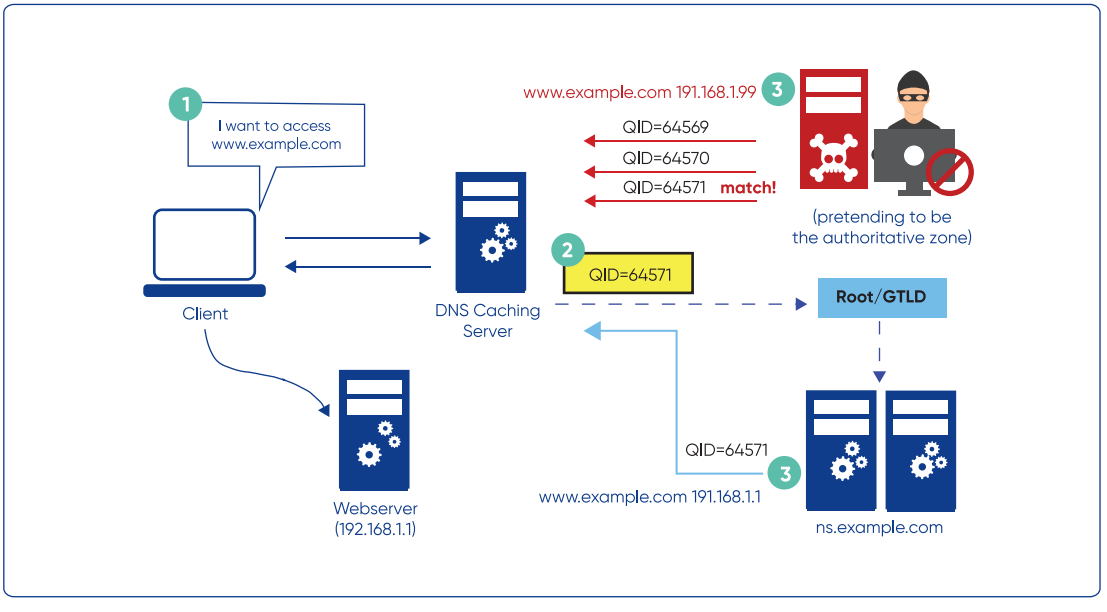
Thay vì thiết lập một DNS Server giả mạo, nếu có thể xâm nhập vào vị trí giữa client và DNS Server, kẻ tấn công có thể ngăn chặn các truy vấn của client gửi đến DNS Server và sau đó gửi gói tin phản hồi với thông tin sai đến client.

Client chỉ chấp nhận các gói tin phản hồi với cùng các thông số đã gửi đi ban đầu như Transaction ID, địa chỉ IP và số cổng (port). Để biết các thông số này, kẻ tấn côn có thể nghe lén để theo dõi, ghi lại các gói tin trong mạng. Sau khi đã có các thông số đầy đủ, kẻ tấn công có thể tạo gói tin phản hồi DNS giả để gửi đến cho client. Nội dung gói tin chứa thông tin sai lệch phục vụ cho mục đích xấu của kẻ tấn công.

Tuy nhiên hạn chế của phương pháp này là gói tin phản hồi của kẻ tấn công phải đến trước gói tin hợp lệ của DNS Server. Nếu gói tin hợp lệ của DNS Server đến trước thì cách tấn công này sẽ không thực hiện được. Đó là do client chỉ chấp nhận gói tin phản hồi nào hợp lệ đến trước và sẽ bỏ qua (ignore) các gói tin đến sau.

Có nhiều cách để thực hiện mục đích này của kẻ tấn công, để tăng khả năng thành công của phương pháp này, kẻ tấn công có thể tiến hành tấn công từ chối dịch vụ (DoS) để làm chậm hoạt động của DNS Server. Do phải theo dõi, ghi lại các gói tin để lấy các thông số của gói tin truy vấn DNS, việc theo dõi các gói tin này khó có thể thực hiện trong môi trường mạng. Do đó, kỹ thuật tấn công ARP spoofing thường được thực hiện trước.

+ **Cách thứ 3: gửi một lượng lớn các phản hồi giả mạo đến client.**



Hình 35: Quá trình tấn công DNS Cache Poisoning

Kỹ thuật tấn công dựa vào số ID DNS spoofing, đòi hỏi kẻ tấn công phải biết chính xác số ID giao dịch giữa client và server. Điều này có thể được thực hiện bằng cách gửi một lượng rất lớn các gói tin phản hồi chứa số Transaction ID khác nhau đến client, hy vọng một trong số các gói tin gửi đến client sẽ hợp lệ.

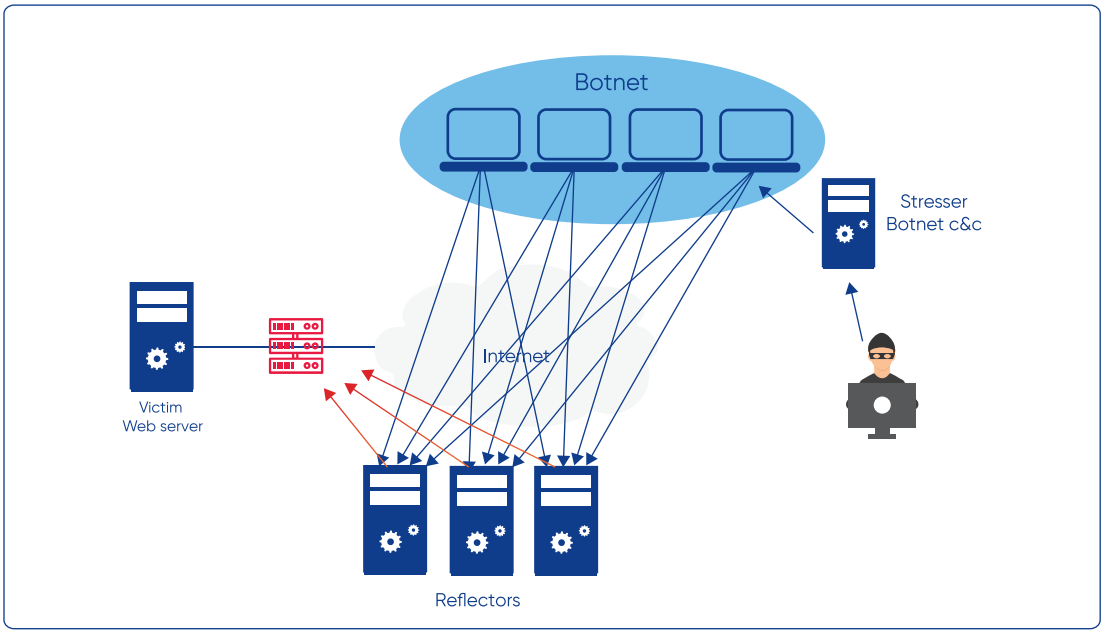
Trên thực tế, số ID này chỉ chiếm 2 byte bộ nhớ, cho nên nó chỉ có tất cả 65525 trường hợp. Vì vậy, bằng cách gửi 65525 gói tin phản hồi (mỗi gói tin có số ID khác nhau), một trong số chúng chắc chắn sẽ phù hợp với số Transaction ID giao dịch giữa client và server, đồng thời có thể làm ngập lụt (food) máy nạn nhân. Với cách tấn công này, kẻ tấn công không cần phải "nghe lén" số Transaction ID giao dịch giữa client và server.

+ **Cách thứ 4: kẻ tấn công gửi một lượng lớn các phản hồi giả mạo đến DNS Server**.

Trong cách thứ 3, kẻ tấn công không thể biết khi nào client thực hiện một truy vấn. Tuy nhiên, trong thực tế, kẻ tấn công có thể tự thực hiện truy vấn và sau đó gửi gói tin phản hồi giả mạo đến DNS Server. Sau đó, DNS Server sẽ chứa thông tin bị đầu độc.

Trong phương pháp này, gói tin phản hồi phải chứa cùng số Transaction ID và số port mà DNS Server nạn nhân đã sử dụng. Để giải quyết vấn đề này, đối với số Transaction ID thì kẻ tấn công sử dụng phương pháp "birthday attack". Trên DNS Server thì cổng nguồn sử dụng hầu như không đổi đối với từng client. Lợi dụng điều này, đầu tiên kẻ tấn công yêu cầu DNS Server nạn nhân phân giải một địa chỉ tên miền nào đó của kẻ tấn công. Trên máy chủ, sau khi nhận được truy vấn kẻ tấn công có thể biết được cổng nguồn nào đang được sử dụng trên DNS Server nạn nhân. Dựa trên sự tính toán này, cùng với số cổng nguồn đã biết, kẻ tấn công thực hiện gửi 65525 truy vấn và 65525 phản hồi giả mạo đến DNS Server nạn nhân. Xác suất thành công của phương pháp tấn công này đạt khoảng 96% tỉ lệ thành công.

2.2. Tấn công từ chối dịch vụ (DoS/DDoS)



Hình 36: Tấn công từ chối dịch vụ DoS/DDoS

Tấn công DOS là những cuộc tấn công nhằm ngăn người dùng hợp pháp truy cập tài nguyên mạng. Thông thường một cuộc tấn công DDoS là một cuộc tấn công sử dụng nhiều tài nguyên mạng làm công cụ để tấn công. Việc sử dụng các nguồn tài nguyên chủ yếu nhằm mục đích khuếch đại, nhưng nó cũng giúp kẻ tấn công ẩn danh và làm phức tạp các biện pháp khắc phục. Hầu hết các cuộc tấn công DDoS tận dụng một mạng máy tính ma "botnet", là một mạng gồm các hệ thống máy tính được kết nối Internet được điều khiển tập trung bởi kẻ tấn công. Botnet có thể có kích thước từ một đến hàng chục triệu hệ thống. Hầu hết các "botnet" sử dụng tài nguyên máy tính bị xâm phạm.

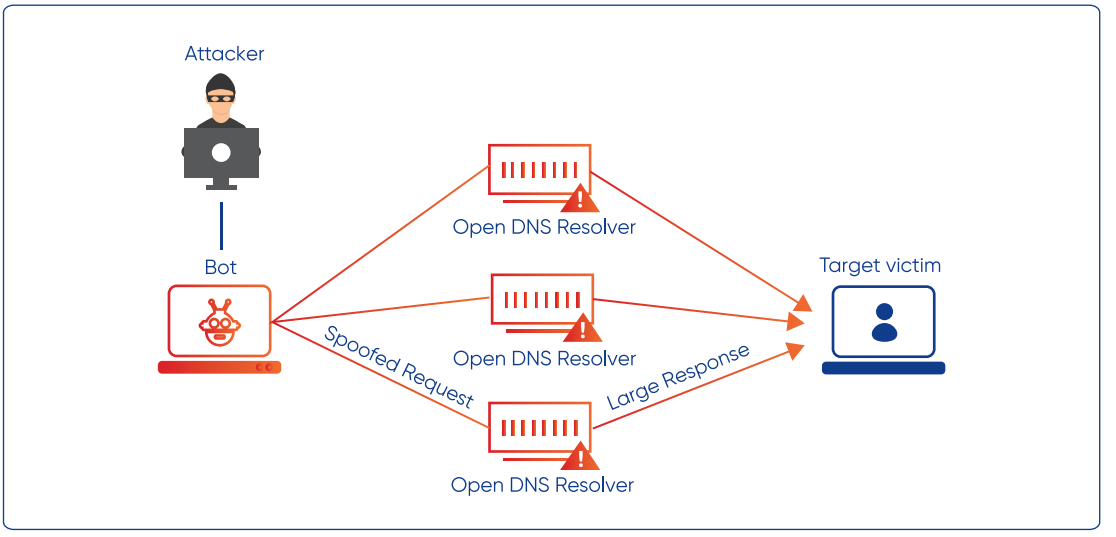
2.3. Tấn công khuếch đại DNS (DNS Amplification Attack)

DNS Amplification Attack là một dạng tấn công từ chối dịch vụ (DDoS) dựa trên phản hồi truy vấn DNS, trong đó kẻ tấn công tận dụng chức năng của các trình phân giải DNS để tiếp cận tấn công máy chủ mục tiêu hoặc mạng với lưu lượng được khuếch đại, làm cho các máy chủ xung quanh không thể tiếp cận.

- **Phương thức hoạt động:**

Bằng cách gửi các truy vấn nhỏ (kích thước gói tin truy vấn nhỏ), sau đó nhận lại các phản hồi lớn hơn (các gói tin phải hồi thường có kích thước lớn hơn), kẻ tấn công đã đạt được mục đích. Thông qua việc ra lệnh cho mỗi bot trong botnet thực hiện các yêu cầu tương tự, kẻ tấn công vừa có thể ẩn danh tránh việc bị phát hiện và cũng đạt được mục đích tấn công.

Do mỗi bot tạo ra các yêu cầu phân giải DNS bằng các địa chỉ IP giả mạo, mà đã được thay đổi thành địa chỉ IP nguồn thật của mục tiêu nạn nhân, mục tiêu sau đó nhận phản hồi từ bộ phân giải DNS. Để tạo ra lưu lượng lớn, kẻ tấn công tạo ra yêu cầu cấu trúc phản hồi lớn từ các trình phân giải DNS.



Hình 37: Tấn công khuếch đại DNS Amplification

Một cuộc tấn công khuếch đại DNS có thể được chia thành 4 bước:

1) Tìm kiếm máy chủ DNS mở: Kẻ tấn công quét internet để tìm các máy chủ DNS có cấu hình mở, cho phép bất kỳ ai gửi yêu cầu DNS và nhận phản hồi.

2) Gửi yêu cầu DNS giả mạo: Kẻ tấn công gửi các yêu cầu DNS tới máy chủ DNS này, nhưng địa chỉ IP nguồn trong yêu cầu được giả mạo để trỏ đến địa chỉ IP của mục tiêu (máy chủ hoặc mạng muốn tấn công).

3) Nhận phản hồi từ máy chủ DNS: Máy chủ DNS nhận yêu cầu và gửi phản hồi đến địa chỉ IP giả mạo (mục tiêu), thay vì gửi về địa chỉ IP thực sự của kẻ tấn công.

4) Khuếch đại lưu lượng tấn công: Mục tiêu nhận được một lượng lớn lưu lượng phản hồi từ nhiều máy chủ DNS khác nhau, dẫn đến tình trạng quá tải và từ chối dịch vụ cho người dùng hợp pháp.

Mỗi một gói truy vấn (UDP) trong các gói truy vấn được gửi tới trình phân giải DNS, thường truyền một tham số như "ANY" để nhận được phản hồi lớn nhất có thể.

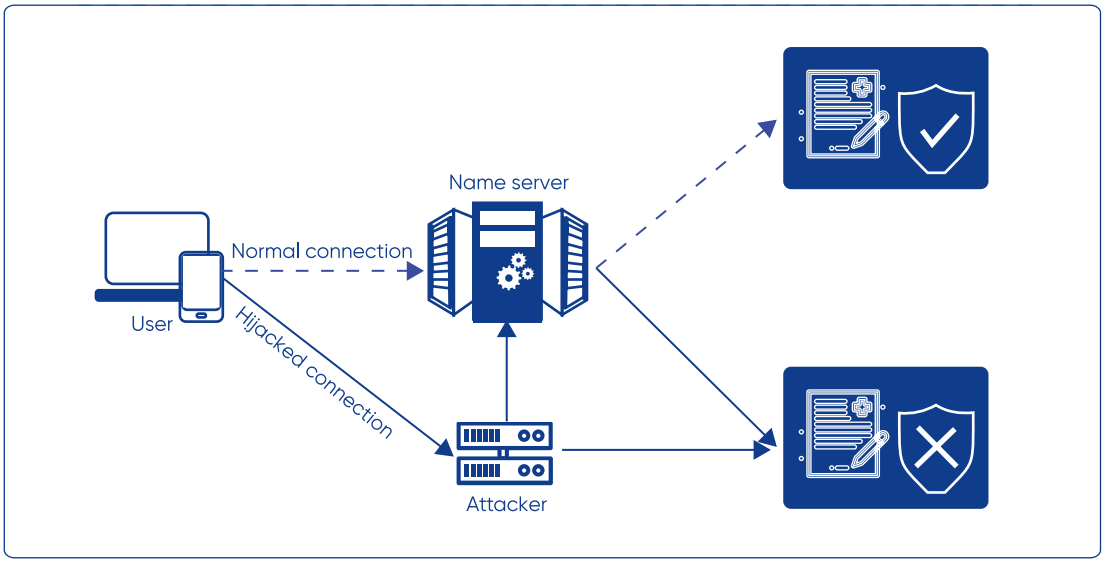
Mặc dù một vài truy vấn không đủ để gây ra tổn hại cho hạ tầng mạng, nhưng khi các truy vấn này được nhân lên nhiều lần, việc khuếch đại dữ liệu mà mục tiêu nhận được rất lớn (tham khảo chi tiết các cuộc tấn công DDoS).

2.4. Tấn công Man-in-the-middle (MitM)

Tấn công Man-in-the-Middle (MitM) là một loại tấn công mạng rất nguy hiểm, trong đó kẻ tấn công chiếm quyền kiểm soát đường truyền giữa hai bên giao tiếp và có thể thao túng hoặc đánh cắp thông tin mà không bị phát hiện. Kẻ tấn công không cần phải trực tiếp phá vỡ hệ thống của người dùng hoặc dịch vụ, mà thay vào đó, chúng làm trung gian trong quá trình trao đổi dữ liệu. Một trong những cách thức phổ biến để thực hiện tấn công MitM là sử dụng ARP Spoofing hoặc DNS Spoofing. Trong ARP Spoofing, kẻ tấn công gửi các gói tin giả mạo trong mạng nội bộ để thay đổi bảng ARP (Address Resolution Protocol), khiến các gói dữ liệu từ người dùng được gửi đến địa chỉ MAC của kẻ tấn công thay vì tới đúng máy chủ đích. Tương tự, trong DNS Spoofing, kẻ tấn công có thể giả mạo phản hồi DNS để thay đổi các địa chỉ IP trả về cho các tên miền hợp pháp, khiến người dùng truy cập vào các trang web giả mạo. MitM có thể dẫn đến việc kẻ tấn công nghe lén thông tin nhạy cảm như tài khoản, mật khẩu, thông tin thẻ tín dụng, hoặc thậm chí thay đổi nội dung các giao dịch trực tuyến mà không bị người dùng phát hiện.

2.5. DNS Hijacking

DNS Hijacking (chiếm quyền điều khiển DNS) là một hình thức tấn công mạng trong đó kẻ tấn công can thiệp vào quá trình phân giải tên miền của hệ thống DNS. Giao thức DNS vốn được thiết kế để ánh xạ tên miền (như vnnic.vn) thành địa chỉ IP (như 192.168.1.1) nhằm đảm bảo các trình duyệt hoặc ứng dụng có thể truy cập được máy chủ lưu trữ nội dung. DNS Hijacking thay đổi quá trình này, chuyển hướng người dùng đến các trang web độc hại hoặc giả mạo nhằm phục vụ các mục tiêu như đánh cắp thông tin cá nhân, lừa đảo tài chính, hoặc phát tán phần mềm độc hại.



Hình 38: Tấn công DNS Hijacking

DNS Hijacking có thể được thực hiện qua nhiều cơ chế khác nhau, tùy thuộc vào cách kẻ tấn công khai thác hệ thống. Dưới đây là các phương pháp phổ biến:

1) Thay đổi cấu hình chương trình phân giải:

Kẻ tấn công sử dụng các phần mềm độc hại hoặc lừa đảo (phishing) để thay đổi cài đặt DNS trên thiết bị của nạn nhân. Khi cấu hình DNS bị thay đổi, tất cả các truy vấn DNS từ thiết bị sẽ được chuyển hướng đến máy chủ DNS do kẻ tấn công kiểm soát. Điều này dẫn đến việc:

- Người dùng bị chuyển đến các trang web giả mạo được thiết kế để đánh cắp thông tin nhạy cảm.
- Các trang web hợp pháp có thể bị giả mạo mà người dùng không nhận ra.

2) Tấn công vào máy chủ DNS:

Kẻ tấn công nhắm mục tiêu vào máy chủ DNS của nhà cung cấp dịch vụ hoặc tổ chức. Bằng cách khai thác các lỗ hổng trong hệ thống, kẻ tấn công có thể thay đổi các bản ghi DNS. Khi đó, bất kỳ người dùng nào sử dụng máy chủ DNS bị xâm nhập đều sẽ bị chuyển hướng đến các trang web do kẻ tấn công kiểm soát. Điều này có thể ảnh hưởng đến một lượng lớn người dùng, gây ra hậu quả nghiêm trọng về bảo mật và kinh doanh.

3) DNS Cache Poisoning

Kẻ tấn công gửi các phản hồi DNS giả mạo đến bộ nhớ đệm (cache) của trình phân giải DNS trước khi trình phân giải nhận được phản hồi hợp pháp từ máy chủ DNS. Điều này dẫn đến việc trình phân giải DNS lưu trữ thông tin sai lệch trong cache. Các truy vấn sau đó sẽ nhận được phản hồi không chính xác từ cache, dẫn đến:

- Người dùng bị chuyển hướng đến các trang web lừa đảo mà không có bất kỳ dấu hiệu đáng nghi ngờ nào.
- Tác động có thể mở rộng vì trình phân giải DNS phục vụ nhiều người dùng.

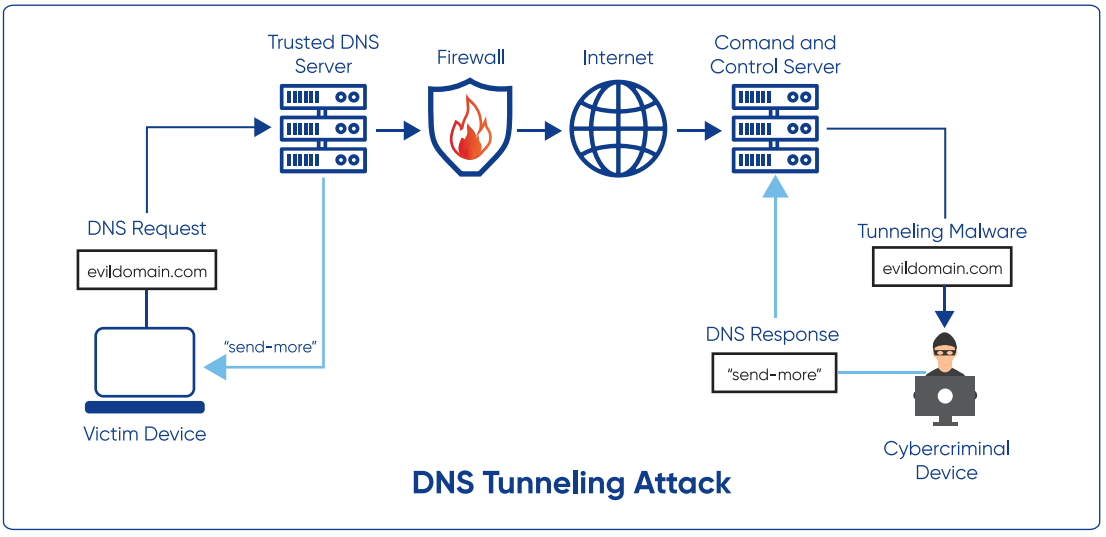
4) Tấn công qua các thiết bị mạng

Kẻ tấn công khai thác lỗ hổng trên router hoặc thiết bị mạng của nạn nhân, thay đổi cài đặt DNS mặc định. Điều này ảnh hưởng đến tất cả các thiết bị kết nối vào mạng, dẫn đến việc chuyển hướng toàn bộ lưu lượng DNS. Đây là một mối nguy hiểm lớn, đặc biệt đối với các tổ chức hoặc hộ gia đình có nhiều thiết bị kết nối.

2.6. DNS Tunneling

DNS Tunneling là một kỹ thuật sử dụng giao thức DNS (Domain Name System) để truyền tải dữ liệu thông qua các gói tin DNS. Giao thức DNS được sử dụng để ánh xạ các tên miền thành địa chỉ IP, nhưng DNS tunneling sử dụng các trường dữ liệu không được sử dụng thông thường trong gói tin DNS để truyền tải dữ liệu bổ sung. DNS Tunneling thường được sử dụng trong các tình huống mà việc truy cập vào Internet bị hạn chế hoặc bị kiểm soát, như trong các mạng cơ quan, doanh nghiệp hoặc các mạng công cộng. Tuy nhiên, DNS Tunneling cũng có thể được sử dụng để thực hiện các cuộc tấn công mạng, bao gồm truy cập trái phép vào mạng hoặc truyền tải thông tin nhạy cảm mà không bị phát hiện.

Cuộc tấn công DNS Tunneling bắt đầu khi người dùng tải phần mềm độc hại xuống máy tính hoặc tin tặc khai thác thành công lỗ hổng trong hệ thống máy tính và cài đặt payload độc hại. Thông thường, những kẻ tấn công sẽ muốn giữ quyền kiểm soát thiết bị, cho phép chúng chạy lệnh hoặc truyền dữ liệu ra ngoài mạng Internet. Để làm điều này, kẻ tấn công cần thiết lập Tunnel - một cách gửi lệnh và nhận dữ liệu từ hệ thống bị xâm nhập đồng thời tránh bị phát hiện bởi các biện pháp bảo mật mạng của nó.



Hình 39: Tấn công DNS Tunneling

Một cuộc tấn công DNS Tunneling có ba giai đoạn:

- **Giai đoạn 1:** Kẻ tấn công đăng ký một tên miền, ví dụ Tunnel.badactor.com. Tên miền trỏ đến máy chủ điều khiển C&C của kẻ tấn công, được sử dụng để liên lạc và đánh cắp dữ liệu.
- **Giai đoạn 2:** Kẻ tấn công lây nhiễm phần mềm độc hại vào máy tính của mục tiêu, sau đó mã hóa thông tin mà kẻ tấn công mong muốn. Giả sử mục tiêu của phần mềm độc hại là truyền danh sách người dùng gồm Alice, Bob và Eve dưới dạng dữ liệu Base64. Các hướng dẫn sẽ trông giống như các chuỗi ký tự như "W2F-saWNlLCBib2lsIGV2ZV0". Do các truy vấn DNS thường ít khi bị tường lửa chặn lọc nên máy tính bị nhiễm được phép gửi truy vấn DNS cho tên miền, trong ví dụ này tên miền được truy vấn sẽ có dạng như sau: "W2FsaWN-lLCBib2lsIGV2ZV0.tunnel. badactor.com".
- **Giai đoạn 3:** Trình phân giải DNS có chức năng phân giải tên miền thành địa chỉ IP chuyển hướng người dùng đến máy chủ C&C của kẻ tấn công. Dữ liệu bị đánh cắp, mã hóa và truyền đến máy chủ C&C.

Kỹ thuật DNS Tunneling cho phép kẻ tấn công thực hiện nhiều hoạt động độc hại, cụ thể:

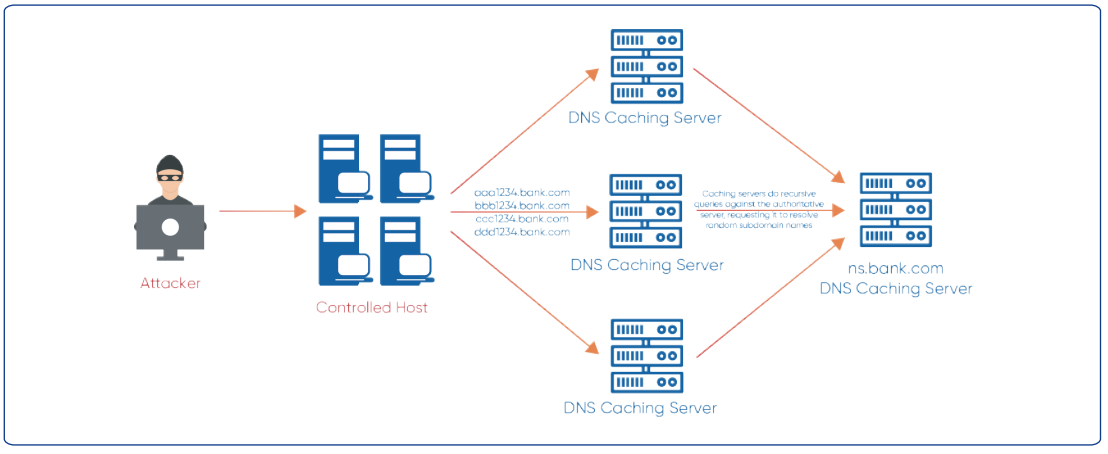
- Cài đặt phần mềm độc hại: Những kẻ tấn công có thể sử dụng DNS Tunneling để cài đặt phần mềm độc hại trên các hệ thống của mục tiêu.
- Thu thập thông tin xác thực: Sau khi có quyền kiểm soát thiết bị, kẻ tấn công có thể sử dụng Keylogger và các phương pháp khác để thu thập thông tin xác thực của người dùng. Những thông tin này có thể được sử dụng để thực hiện các cuộc tấn công bổ sung hoặc được bán trên web "đen".
- Mô hình hóa hệ thống mạng: Các truy vấn DNS từ bên trong mạng bị nhiễm có thể giúp kẻ tấn công xây dựng bản đồ mạng, xác định hệ thống và tài sản có giá trị cao trong hệ thống mạng của mục tiêu.
- Lọc dữ liệu: Kẻ tấn công có thể sử dụng DNS Tunneling để truyền dữ liệu ra khỏi mạng, bao gồm cả thông tin nhạy cảm hoặc bí mật của người dùng.
- Điều khiển các thiết bị: Với khả năng kiểm soát thiết bị bị nhiễm, kẻ tấn công có thể kích hoạt các mối đe dọa khác như tấn công DDoS.

Ngoài ra, còn có nhiều hình thức tấn công DNS khác, dưới đây là tóm tắt một số hình thức tấn công phổ biến khác:

- Phantom Domain Attack: là một loại tấn công mạng mà kẻ tấn công tạo ra hoặc sử dụng các tên miền giả mạo (phantom domains) để thực hiện các hoạt động độc hại. Đây là một chiến thuật thường được sử dụng trong các cuộc tấn công lừa đảo, tấn công chiếm đoạt tài khoản, hoặc để phát tán phần mềm độc hại.

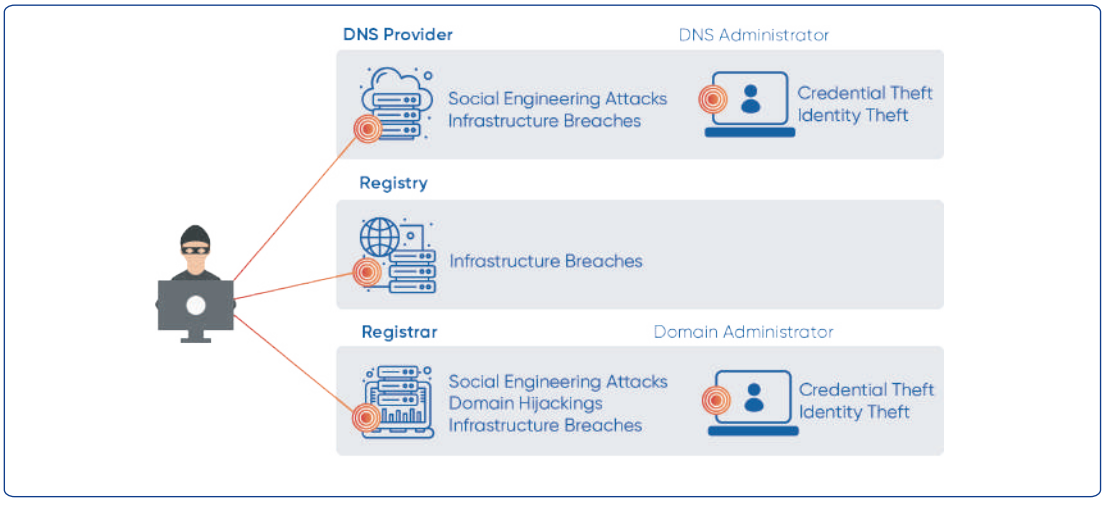
Hình 40: Tấn công Phantom Domain Attack

- Random Subdomain Attack: là một loại tấn công mạng trong đó kẻ tấn công tạo ra và kiểm tra ngẫu nhiên các subdomain (tên miền con) của một tên miền chính nhằm tìm kiếm thông tin hoặc lỗ hổng bảo mật. Kỹ thuật này thường được sử dụng để phát hiện các tài nguyên không được bảo vệ hoặc các dịch vụ mà quản trị viên có thể đã quên bảo mật.



Hình 41: Tấn công Random Subdomain Attack

- Domain Hijacking: Chiếm đoạt tên miền là một hành vi mà kẻ tấn công chiếm quyền kiểm soát một tên miền một cách bất hợp pháp. Đây là một mối đe dọa nghiêm trọng trong quản lý tên miền, có thể dẫn đến việc mất quyền truy cập vào các tài nguyên và dịch vụ trực tuyến của tổ chức hoặc cá nhân.



Hình 42: Tấn công Domain Hijacking

3. DNS và Malware

3.1. Mối liên hệ giữa Cyber Kill Chain và DNS

Cyber Kill Chain là một mô hình được phát triển bởi Lockheed Martin nhằm mô tả các bước trong một cuộc tấn công mạng, gồm các bước chính sau:

- Reconnaissance (Trinh sát)
- Weaponization (Vũ khí hóa)
- Delivery (Phân phối)
- Exploitation (Khai thác)
- Installation (Cài đặt)
- Command and Control (C2 - Điều khiển và Kiểm soát)
- Actions on Objectives (Hành động theo mục tiêu)

DNS không đóng vai trò trực tiếp trong mọi bước của Cyber Kill Chain, nhưng nó lại là yếu tố thiết yếu trong hầu hết các bước. Chi tiết chúng ta cùng phân tích từng bước để thấy rõ vai trò của DNS.

3.1.1. Reconnaissance (Trinh sát)

Trong bước này, kẻ tấn công thu thập bất kỳ thông tin nào chúng có thể thu thập được về mục tiêu, chẳng hạn như địa chỉ email, thông tin IP, và các ứng dụng, dịch vụ trên Internet khác. DNS, với vai trò là một cơ sở dữ liệu công khai chứa các thông tin về tên miền, địa chỉ IP tương ứng, trở thành mục tiêu chính trong giai đoạn này. Bằng cách khai thác DNS, kẻ tấn công có thể thu thập được:

- Tên miền và địa chỉ máy chủ thư điện tử (Mail servers): Kẻ tấn công có thể tìm ra địa chỉ của các máy chủ thư điện tử, điều này cho phép chúng hiểu rõ hơn về hạ tầng mạng.
- Không gian địa chỉ IP (Address spaces): Bao gồm cả các dải địa chỉ công cộng (public) và riêng tư (private), từ đó giúp kẻ tấn công xác định được quy mô và mô hình mạng.
- Tên máy chủ (Host names): Các tên máy chủ có thể tiết lộ thông tin về hệ thống hoặc phần mềm đang hoạt động (ví dụ: exchange01.vnnic.vn).
- Tên miền Active Directory (AD).

3.1.2. Weaponization (Vũ khí hóa)

Thông thường, kẻ tấn công tận dụng các lỗ hổng phần mềm và phần cứng để triển khai cài đặt các phần mềm độc hại. DNS được sử dụng để hỗ trợ trong việc phát tán và thực thi. Tuy nhiên, DNS trở thành một yếu tố quan trọng trong các cuộc tấn công lên các máy chủ DNS hoặc lợi dụng các trình phân giải DNS public để tạo ra lưu lượng truy cập trong các cuộc tấn công từ chối dịch vụ (DoS/DDoS).

3.1.3. Delivery (Phát tán)

Kẻ tấn công phát tán các phần mềm độc hại đến thiết bị mục tiêu, thường thông qua giao thức web (HTTP hoặc HTTPS). Tuy nhiên việc phát tán mã độc thông qua hệ thống DNS ngày các trở nên phổ biến hơn, thậm chí bao gồm cả việc sử dụng DNS mã hóa (được mô tả chi tiết trong phần Mã hóa DNS).

Bất kỳ việc phát tán mã độc qua kênh nào thì quá trình phát tán đều phụ thuộc vào khả năng phân giải tên miền của DNS. Điều này đặt DNS vào vị trí trung tâm của quá trình phát tán phần mềm độc hại.

3.1.4. Exploitation (Khai thác)

Kẻ tấn công khai thác một lỗ hổng để thực thi mã độc trên hệ thống của nạn nhân, chẳng hạn như một lỗ hổng trong phần mềm máy chủ thư điện tử, trong bước này thì giao thức/dịch vụ DNS cũng có thể bị khai thác.

3.1.5. Installation (Cài đặt)

Kẻ tấn công cài đặt phần mềm độc hại trên thiết bị, hệ thống mục tiêu. Trong nhiều trường hợp, bước này không trực tiếp liên quan đến DNS, phần mềm độc hại có thể đã được tải xuống hoặc truyền qua DNS trước đó, nhưng việc cài đặt thực tế trên thiết bị mục tiêu thường diễn ra mà không cần đến DNS.

3.1.6. Command and Control (C2 - Điều khiển và Kiểm soát)

Khi các thiết bị đã bị xâm nhập, kẻ tấn công thiết lập một kênh điều khiển để chiếm quyền kiểm soát, điều khiển từ xa thiết bị của nạn nhân. Các kênh điều khiển được triển khai thông qua giao thức/hệ thống DNS ngày càng phổ biến.

3.1.7. Actions on Objectives (Hành động trên các mục tiêu)

Trước đây các cuộc tấn công tập trung làm suy giảm hoặc gián đoạn các dịch vụ DNS, chẳng hạn như thông qua một cuộc tấn công DDoS nhằm làm gián đoạn, ngưng trệ toàn bộ hệ thống mạng. Hiện nay, ngoài mục tiêu này, việc tấn công mạng còn nhằm gây ra thiệt hại lớn hơn nhiều bằng cách sử dụng DNS để phát tán hoặc che giấu phần mềm độc hại và ransomware.

Như vậy, có thể thấy rằng DNS có vai trò rất lớn, được sử dụng trong hầu hết các bước của một cuộc tấn công mạng.

3.2. Cách phần mềm độc hại sử dụng DNS

Hai mục đích chính khi phần mềm độc hại lợi dụng hoặc sử dụng giao thức/dịch vụ DNS là nhằm:

- Xác định điều kiện, thời điểm phù hợp để đưa ra quyết định tấn công. Ví dụ: mã độc WannaCry sử dụng DNS để kiểm tra xem liệu có an toàn để kích hoạt cuộc tấn công hay không.
- Tìm kiếm máy chủ để tải thêm các tệp mã độc thực thi. Ví dụ: mã độc Black KingDom sử dụng DNS để định vị các máy chủ nhằm tải xuống thêm các tệp độc hại.

Phần mềm độc hại cũng sử dụng giao thức/dịch vụ DNS để tải xuống các tệp thực thi độc hại thông qua kỹ thuật DNS Tunneling.

4. Các biện pháp bảo mật

Hiện nay, có nhiều giải pháp bảo mật khác nhau nhằm bảo vệ và tăng cường an toàn cho hệ thống DNS. Mỗi giải pháp hướng đến một vấn đề cụ thể và có những phương pháp tiếp cận riêng nhằm đối phó với các mối đe dọa an ninh mạng, đặc biệt là những mối đe dọa lợi dụng chính nền tảng DNS. Trong số đó, DNSSEC nổi bật là giải pháp bảo mật toàn diện nhất, cung cấp khả năng xác thực và đảm bảo tính toàn vẹn của dữ liệu DNS (được phân tích chuyên sâu trong mục DNSSEC). Các giải pháp bảo mật quan trọng như DNS Firewall & RPZ, giám sát và phân tích lưu lượng DNS, Blocking DGA đóng vai trò then chốt trong việc phát hiện và ngăn chặn các tấn công lợi dụng DNS sẽ được phân tích chi tiết trong phần dưới đây. Ngoài ra, các công nghệ mã hóa truy vấn DNS như DNS-over-TLS (DoT) và DNS-over-HTTPS (DoH), với mục tiêu bảo vệ tính bảo mật và quyền riêng tư cho người dùng, sẽ được trình bày cụ thể trong phần Mã hóa DNS.

Tất cả các giải pháp này, khi được kết hợp hiệu quả, sẽ tạo ra một hệ thống phòng thủ nhiều lớp, bảo vệ toàn diện và chủ động cho hạ tầng DNS trước những cuộc tấn công tinh vi nhất.

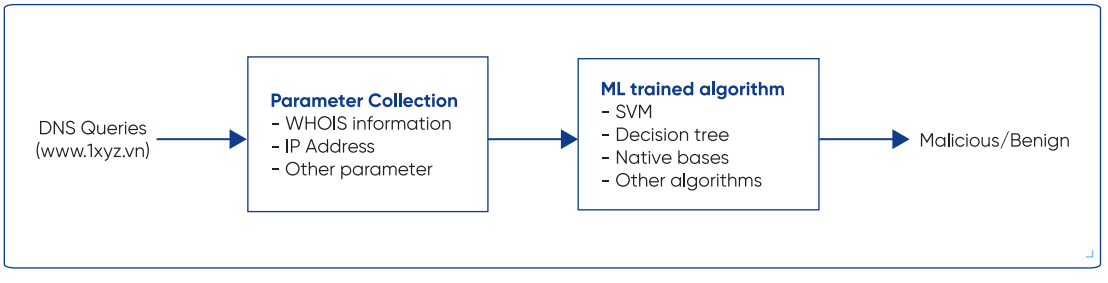
4.1. Giải pháp DNS Firewall & RPZ

4.1.1. Giới thiệu

Các cuộc tấn công dựa trên hệ thống, giao thức DNS như sử dụng botnet là một trong những mối đe dọa bảo mật lớn nhất, cho phép huy động mạng lưới hàng ngàn, thậm chí hàng triệu máy được điều khiển từ xa thực hiện một cuộc tấn công, do đó làm tăng đáng kể xác suất thành công và gây ra các thiệt hại vô cùng lớn. Để tránh việc bị các cơ quan chức năng gỡ bỏ các mạng botnet, các kẻ tấn công thông thường sẽ sử dụng thuật toán tạo miền DGA (Domain Generation Algortithm). Với kỹ thuật này cho phép kẻ tấn công có thể tạo ra các tên miền ngẫu nhiên thay đổi theo thời gian. Kỹ thuật DGA sử dụng 4 tham số chính gồm: số học, hàm băm, danh sách từ và hoán vị. Kết hợp giữa đầu vào là danh sách các đuôi tên miền (ví dụ: .com.vn, .net.vn, .vn, ...) với các chuỗi số hoặc ký tự để tạo ra danh sách tên miền ngẫu nhiên (ví dụ: 1xy.com.vn, 2yz.com.vn, ...). Do tính ngẫu nhiên của các tên miền này nên rất khó để xác định xem một tên miền nhất định có độc hại hay không. Kỹ thuật đảo ngược (Reverse engineering - RE) thường được sử dụng để xác minh cách thức các tên miền này được tạo và sau đó phá hủy thông tin liên lạc, mặc dù RE mất nhiều thời gian để các tên miền hoạt động trong thời gian dài. Trong trường hợp này, việc ứng dụng công nghệ học máy (machine learning - ML) để cải thiện việc phân loại tên miền độc hại và không độc hại là điều cần thiết.

Bản chất của giải pháp DNS Firewall là sử dụng nguyên tắc kiểm soát truy vấn DNS thông qua việc định nghĩa các chính sách phản hồi truy vấn cho các zone tên miền (Response Policy Zone), trong trường hợp này thì DNS Firewall còn được gọi là DNS RPZ. Việc sử dụng công nghệ học máy (ML), để chủ động xác định các mối đe dọa có thể có thông qua phân tích lưu lượng DNS, kết hợp với phương pháp DNS RPZ giúp cải thiện việc phát hiện các tên miền độc hại.

Đối với giải pháp sử dụng ML, hệ thống sẽ phân tích từng truy vấn DNS để thu thập thông tin về tên miền và sử dụng thông tin đó làm đầu vào cho quá trình xử lý sau này. Ở bước này, các thông số như thông tin WHOIS, địa chỉ IP và tên miền con, ... sẽ được thu thập, phân tích. Sau khi thu thập tham số, dữ liệu sẽ được phân loại, xử lý ứng dụng công nghệ học máy (ML). Kết quả xử lý sẽ được sử dụng để xác định xem tên miền có độc hại hay không. Quá trình này có thể được khái quát hóa như hình vẽ dưới đây.



Hình 43: Ứng dụng ML phân tích truy vấn DNS phát hiện mã độc

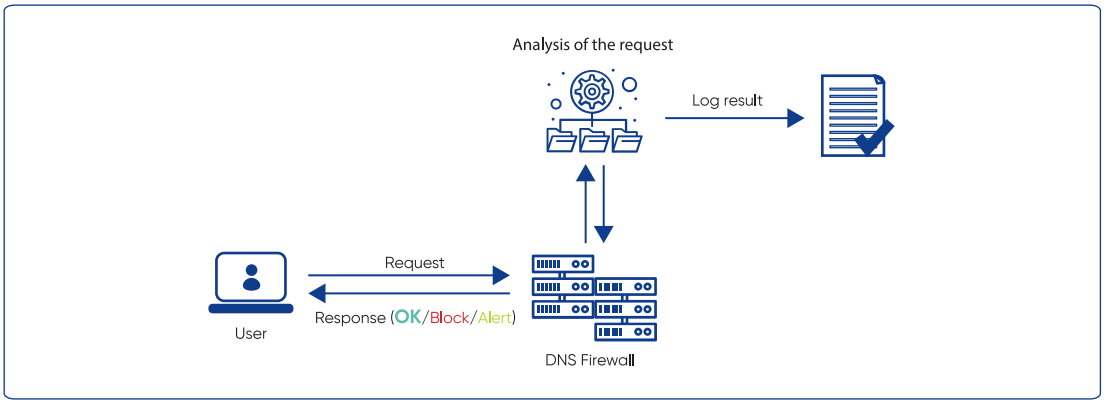
Về tổng thể, giải pháp DNS Firewall đầy đủ sẽ sử dụng tích hợp 2 chức năng:

- RPZ để định nghĩa chính sách dựa trên danh sách chặn/cho phép.
- Phân tích lưu lượng DNS, trong đó đặc biệt có ứng dụng học máy (ML).

Với giải pháp tổng thể như trên, có thể chặn quyền truy cập vào các tên miền đã được xác định từ trước (RPZ sử dụng blacklist, whitelist) là độc hại và các tên miền khác chưa được liệt kê trong danh mục nhưng có khả năng cao là tên miền độc hại (Phân tích lưu lượng).

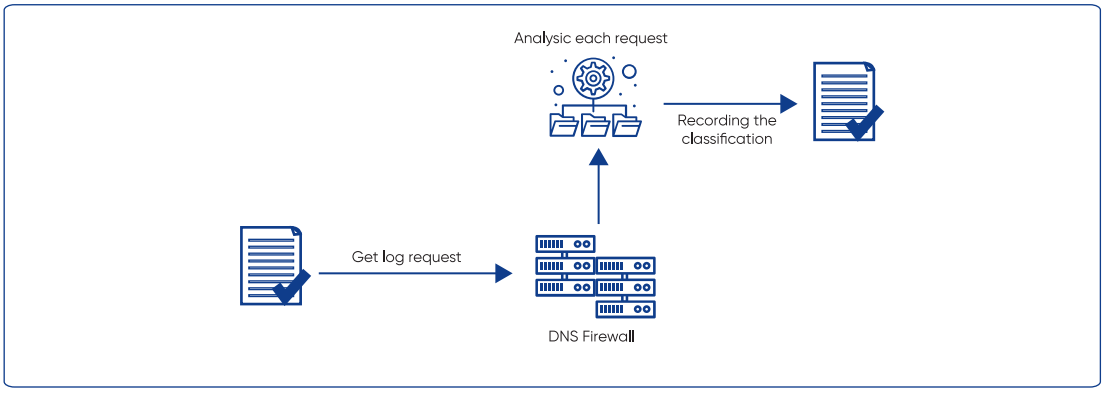
Giải pháp DNS Firewall sẽ được triển khai ở hai chế độ hoạt động riêng biệt: trực tuyến (in-band) và ngoại tuyến (out-band). Chế độ in-band thường được sử dụng để phân tích hoạt động DNS một cách chủ động và chế độ out-band thường được sử dụng trong phân tích hoạt động DNS một cách thụ động (copy lưu lượng, vết truy vấn DNS và phân tích, xử lý sau).

- In-band: Như được minh họa trong hình vẽ bên dưới, trong mô hình này các yêu cầu phân giải DNS được phân tích theo thời gian thực. Do đó cho phép xác định xem tên miền được yêu cầu có độc hại hay không và chặn hoặc cảnh báo sớm.



Hình 44: Mô hình triển khai DNS Firewall in-band

- Out-band: Như được minh họa trong hình vẽ bên dưới, trong mô hình này DNS Firewall sẽ chỉ phân tích định kỳ lưu lượng truy vấn DNS. Do đó việc phát hiện, chặn lọc, cảnh báo tên miền là độc hại thường không theo thời gian thực mà có độ trễ. Tuy nhiên, với mô hình này sẽ không làm ảnh hưởng đến tải quá trình xử lý truy vấn và hoạt động của hệ thống DNS.



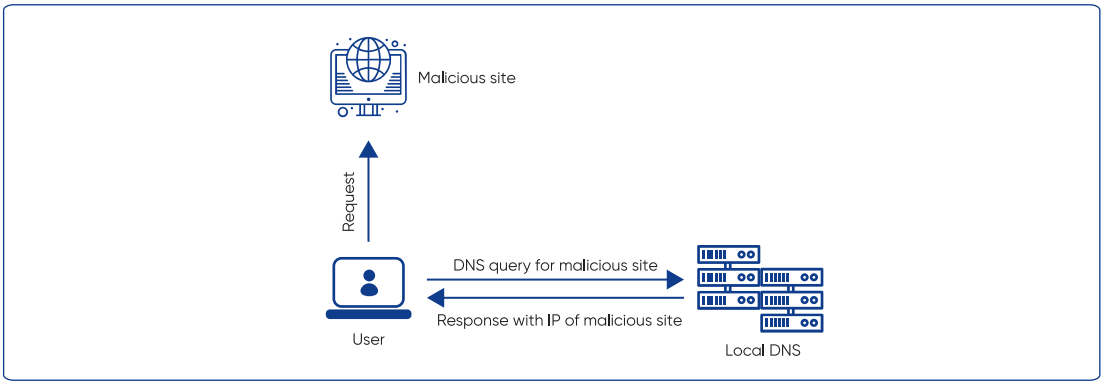
Hình 45: Mô hình triển khai DNS Firewall out-band

Tùy vào điều kiện, có thể triển khai giải pháp DNS Firewall sử dụng 1 trong 2 chức năng trên đều được. Trong đó, việc triển khai DNS Firewall sử dụng RPZ là khả thi, có thể thực hiện được ngay. Việc triển khai DNS Firewall sử dụng học máy là khá phức tạp, cần có đội ngũ làm về khoa học, phân tích dữ liệu (data analyst, data engineer), phát triển phần mềm (coder), hệ thống (system) để nghiên cứu, phát triển, ứng dụng công nghệ học máy trong phân tích lưu lượng DNS.

4.1.2. Mô hình DNS Firewall (DNS RPZ)

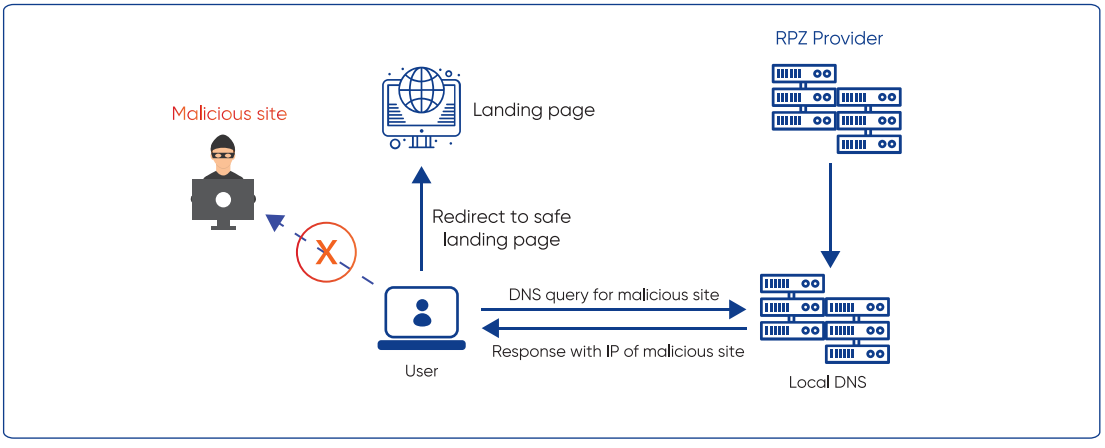
Đối với hệ thống DNS không sử dụng RPZ: Việc kết nối, truy cập dịch vụ sử dụng tên miền từ người dùng diễn ra theo cơ chế như đã trình bày ở trên. Quá trình này có thể tóm tắt gồm các bước chính như sau: Người dùng cuối

cố gắng truy cập ứng dụng, dịch vụ trên Internet (ví dụ: website), chương trình trình resolver trên máy tính người dùng sẽ kết nối, truy vấn đến máy chủ DNS gốc, sau đó là máy chủ DNS cấp cao nhất, ... và cuối cùng là máy chủ của ứng dụng, dịch vụ. Yêu cầu truy cập ứng dụng, dịch vụ của người dùng sẽ diễn ra bất kể ứng dịch, dịch vụ (tên miền, website) đó có độc hại hay không.



Hình 46: Hệ thống DNS không sử dụng RPZ

Đối với hệ thống DNS sử dụng RPZ (DNS RPZ): Bản chất của giải pháp DNS RPZ là sử dụng nguyên tắc kiểm soát truy vấn DNS thông qua việc định nghĩa các chính sách phản hồi truy vấn cho các zone tên miền (Response Policy Zone), trong trường hợp này thì DNS Firewall còn được gọi là DNS RPZ.



Hình 47: Hệ thống DNS sử dụng RPZ

Hệ thống tường lửa mạng truyền thống mặc dù sử dụng các công nghệ độc quyền và phức tạp nhưng vẫn không có khả năng trong việc phát hiện và chặn lọc các mối nguy hại và đe dọa dựa trên tên miền và giao thức DNS. Do vậy, DNS RPZ sẽ đóng vai trò quan trọng trong việc phát hiện, ngăn chặn mã độc dựa trên nền tảng hệ thống DNS. Mỗi truy vấn DNS sẽ được kiểm tra và lọc theo danh sách từ chối (blacklist), danh sách này sẽ bao gồm các thông tin: địa chỉ IP, máy chủ, tên miền (trang web độc hại). Yêu cầu truy cập đến trang web hoặc dịch vụ trên Internet sẽ bị từ chối nếu quá trình kiểm tra, lọc tìm thấy thông tin trong danh sách này.

Tổng quát, hệ thống DNS RPZ sẽ gồm các thành phần chức năng cơ bản như sau:

- RPZ Provider (Feed): Đây chính là cơ sở dữ liệu, cung cấp thông tin, dữ liệu, danh sách để chặn lọc. Ngoài các dữ liệu do cán bộ quản trị tự cập nhật thì có thể sử dụng các cơ sở dữ liệu mở của bên thứ ba hoặc thương mại.
- Trang landing page: Là trang thông báo cho người sử dụng khi truy cập từ máy tính của người sử dụng đến một trang web có mã độc được hệ thống phát hiện và chuyển hướng đến trang landing page này.
- Chức năng thông báo nhiễm mã độc: Người sử dụng được thông báo kịp thời về các hệ thống có thể bị lây nhiễm thông qua các thông báo bảo mật.

Hoạt động của hệ thống DNS RPZ dựa trên việc định nghĩa các chính sách/luật (rule) phản hồi truy vấn cho các zone tên miền (RPZ). Mỗi chính sách sẽ bao gồm các dấu hiệu "Trigger" và hành động "Action" tương ứng. Mỗi chính sách có thể sử dụng 1 trong số 5 dấu hiệu nhận biết và chỉ định 1 trong số 8 hành động tương ứng, cụ thể như sau:

- Dấu hiệu nhận biết (Response Policy Triggers):
+ Theo tên miền truy vấn [QNAME].
+ Theo địa chỉ IP có thể có trong một phản hồi DNS [RPZ-IP].
+ Theo tên miền hoặc địa chỉ IP của một máy chủ tên miền Authoritative DNS Server [RPZ-NSDNAME và RPZ-NSIP].
+ Theo địa chỉ IP của client [RPZ-CLIENT-IP].
- Hành động (Response Policy Actions):
+ Trả về phản hồi DNS với "tên miền không tồn tại" [NXDOMAIN].
+ Trả về phản hồi DNS với "tên miền tồn tại nhưng không có bất kỳ thông tin bản ghi nào" [NODATA].
+ Chuyển hướng người dùng tới một tên miền hoặc bất kỳ tên miền con nào thông qua một CNAME [ví dụ: CNAME vnnic.vn].
+ Thay thế phản hồi bằng dữ liệu đã được chỉ định [Local Data].
+ Yêu cầu client phải gửi lại truy vấn thông qua giao thức TCP. [CNAME rpz-tcp-only].
+ Không áp dụng bất kỳ chính sách nào, thực hiện phân giải như thông thường [DISABLED, CNAME rpz-passth-ru].
+ Loại bỏ truy vấn, không có bất kỳ phản hồi nào đến Client [CNAME rpz- drop].

Hiện nay, DNS RPZ là tính năng được tích hợp trong các phần mềm dịch vụ DNS. Hầu hết phần mềm DNS mã nguồn mở và thương mại đều đã hỗ trợ tính năng này. Các sản phẩm an toàn bảo mật của một số hãng an toàn thông tin cũng được cài đặt, tích hợp sẵn DNS RPZ. Đơn cử như sau:

STT	NHÀ CUNG CẤP	SẢN PHẨM	MÔ TẢ
1	Akami	AnswerX	Thiết bị phần cứng tích hợp DNS RPZ
2	BlueCat	BlueCat DNS	Thiết bị phần cứng tích hợp DNS RPZ
3	EfficientIP	SolidServer	Thiết bị phần cứng tích hợp DNS RPZ
4	InfoBlox	DNS Firewall	Thiết bị phần cứng tích hợp DNS RPZ
5	ISC	BIND 9	RPZ tích hợp, hỗ trợ trong các phiên bản phần mềm Bind từ 9.8.
6	Knot	policy.rpz module	Thiết bị phần cứng tích hợp DNS RPZ
7	NLnet Labs	NLnet Labs Unbound	RPZ tích hợp, hỗ trợ trong các phiên bản phần mềm Unbound từ 1.10.
8	PowerDNS	PowerDNS Recursor	RPZ tích hợp, hỗ trợ trong các phiên bản phần mềm PowerDNS Recursor từ 4.4.0.

4.2. Giải pháp giám sát, phân tích lưu lượng DNS

4.2.1. Giới thiệu

Phân tích dữ liệu bao gồm việc áp dụng các phương pháp và kỹ thuật để khai thác, xử lý và tìm ra thông tin hữu ích từ dữ liệu. Thông qua các công cụ và kỹ thuật phân tích, chúng ta có thể phát hiện ra các xu hướng, mô hình và mối quan hệ trong dữ liệu, từ đó tạo ra thông tin giá trị và cung cấp cơ sở để đưa ra quyết định và dự đoán. Phân tích dữ liệu đóng vai trò quan trọng trong nhiều lĩnh vực trong cuộc sống đặc biệt là kỹ thuật.

Quy trình phân tích dữ liệu bắt đầu bằng việc thu thập thông tin từ nhiều nguồn khác nhau, bao gồm cả cơ sở dữ liệu, tệp tin, và nguồn dữ liệu trực tuyến. Sau đó, dữ liệu được xử lý để chuẩn hóa, làm sạch, và loại bỏ các giá trị không hợp lệ hoặc thiếu sót. Tiếp theo, dữ liệu được biến đổi và chuyển đổi thành định dạng phù hợp để phục vụ cho mục đích phân tích. Cuối cùng, các phương pháp phân tích thống kê, khai phá dữ liệu, và học máy được áp dụng để tìm ra thông tin, xu hướng, và kiến thức hữu ích từ dữ liệu số hóa này. Quy trình này đóng vai trò quan trọng trong việc đưa ra quyết định, dự đoán, và phát triển chiến lược trong nhiều lĩnh vực khác nhau.

4.2.2. Các phương pháp, cách tiếp cận trong giám sát phân tích dữ liệu DNS

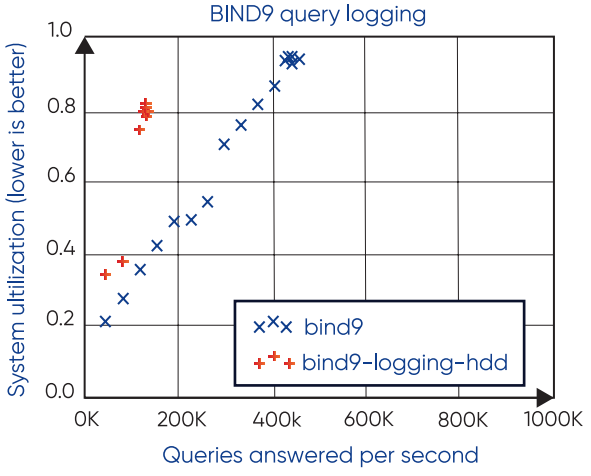
Như đã giới thiệu ở trên, việc phân tích dữ liệu là một nội dung rất rộng, bao gồm rất nhiều các hành động, công việc và thu thập từ rất nhiều nguồn thông tin, dữ liệu liên quan khác nhau. Nhưng trong phạm trù lĩnh vực DNS, đã được quan tâm nghiên cứu, ứng dụng trên thế giới để hỗ trợ khai thác dữ liệu, phục vụ cho giám sát vận hành và đảm bảo an toàn an ninh cho các hệ thống.

Hiện nay có 02 phương pháp tiếp cận chính và phổ biến, được sử dụng rộng rãi hiện nay cho việc phân tích giám sát dữ liệu hoạt động của hệ thống DNS gồm: Phân tích và giám sát dựa vào nhật ký (log) truy vấn/phản hồi truy vấn DNS; Phân tích và giám sát dựa trên phân tích lưu lượng DNS. Đây là 02 hướng tiếp cận hoàn toàn khác nhau và mang lại các giá trị khác biệt. Chi tiết theo các phân tích, nghiên cứu dưới đây.

a) Phân tích và giám sát dựa vào nhật ký (log) truy vấn/phản hồi truy vấn DNS

Phương pháp phân tích và giám sát hoạt động hệ thống DNS dựa vào nhật ký (log) truy vấn/phản hồi truy vấn DNS là phương pháp được sử dụng khá lâu đời và cơ bản. Bởi việc ghi nhật ký và giám sát DNS rất quan trọng, giám sát dựa vào nhật ký DNS có thể cho phép phân tích và phát hiện lưu lượng truy cập độc hại (C&C), đồng thời có quyền xem một số thông tin quan trọng để có thể đánh giá, phát hiện sớm các kết nối không phù hợp. Kết hợp với một số giải pháp phát hiện tấn công DNS khác, tạo ra nguồn dữ liệu rất có giá trị được sử dụng trong quá trình ứng phó sự cố. Tuy nhiên, phương pháp này sẽ tồn tại một số nhược điểm như sau:

Việc ghi nhật ký DNS phải "trả giá" bằng hiệu năng của toàn bộ hệ thống. Do mọi tác vụ ghi nhật ký đều yêu cầu hệ thống ghi một mục vào đĩa (ngoài ra còn phải định dạng đúng định dạng nhật ký). Đây được xem như một hoạt động I/O "chậm" và có thể làm ảnh hưởng, giới hạn số lượng truy vấn DNS tối đa mà hệ thống có thể trả lời. Một nghiên cứu của Farsight Security cho thấy sự khác biệt khi chạy BIND9 có hoặc không có ghi nhật ký truy vấn.



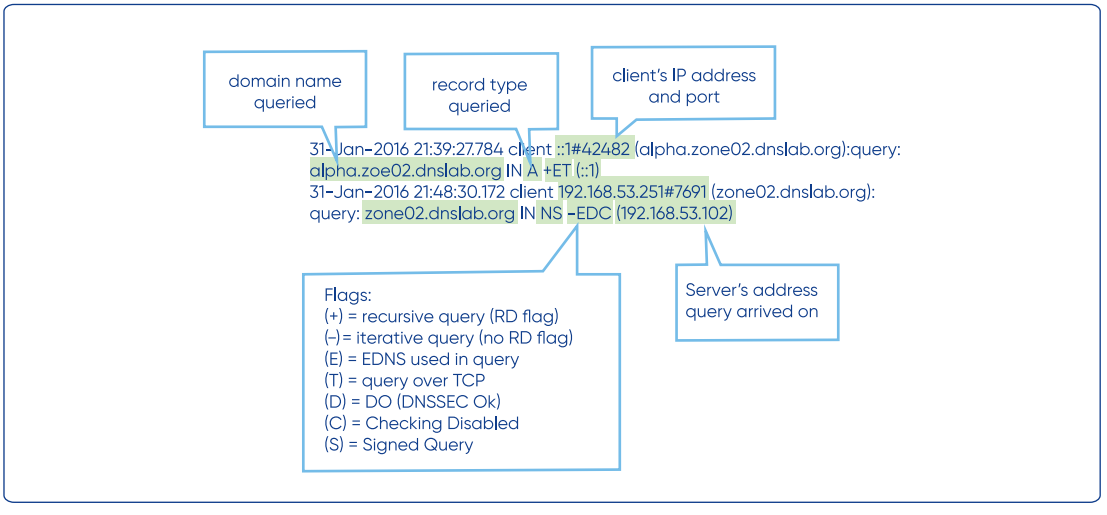
Hình 48: Hiệu năng phần mềm BIND9 khi tắt & bật logging

Mỗi một phần mềm DNS đều có đặc tính cấu trúc và định dạng dòng nhật ký (log) truy vấn DNS khác nhau và chứa đựng các trường thông tin khác nhau. Tuy nhiên các phần mềm này đều có một đặc điểm chung là không ghi lại nhật ký phản hồi truy vấn DNS của hệ thống, máy chủ DNS, do đó mọi thông tin liên quan đến phản hồi truy vấn đều không được thu thập, thống kê.

Một số phần mềm DNS được sử dụng phổ biến hiện nay như: BIND9, PowerDNS, NSD, Unbound, Knot, ...

Dưới đây là một số ví dụ về định dạng nhật ký (log) truy vấn DNS của một số phần mềm DNS:

- **Phần mềm BIND9:**



Hình 49: Định dạng dòng nhật ký truy vấn DNS phần mềm BIND9

Trong định dạng dòng nhật ký (log) truy vấn trên của phần mềm BIND9 có 06 trường thông tin quan trọng:

+ Mốc thời gian
+ Địa chỉ IP và cổng của nguồn truy vấn
+ Tên miền truy vấn
+ Loại bản ghi truy vấn
+ Các cờ truy vấn (+, -, E, T, D, C, S)
+ Địa chỉ IP máy chủ DNS nhận truy vấn

- **Phần mềm PowerDNS:**

Đối với phần mềm PowerDNS chỉ có các trường thông tin chính như sau:

+ Mốc thời gian
+ Địa chỉ IP của nguồn truy vấn
+ Tên miền truy vấn
+ Loại bản ghi truy vấn
+ Các cờ truy vấn (do)
+ Địa chỉ IP máy chủ DNS nhận truy vấn
+ Kích thước đệm (buffsize)
+ Loại phản hồi (Cache HIT/MISS)

b) Phân tích và giám sát dựa trên phân tích lưu lượng DNS

Tình hình mạng Internet đã trở nên càng ngày càng phức tạp trong những năm qua dẫn tới việc thiết kế các công cụ và phần mềm có khả năng mở rộng để phân tích và giám sát lưu lượng mạng (Network Traffic Monitoring and Analysis - NTMA) trở nên quan trọng hơn và khó khăn hơn và việc phân tích giám sát dựa trên nhật ký (log) của hệ thống không còn là ưu tiên, sự lựa chọn số một mà thay vào đó là các giải phaspm ứng dụng phân tích và giám sát lưu lượng mạng quan trọng như phát hiện các bất thường, các cuộc tấn công mạng và xâm nhập mạng, yêu cầu cơ chế phân tích trực tuyến với hàng nghìn các sự kiện mỗi giây, cũng như các kỹ thuật hiệu quả để phân tích ngoại tuyến (offline) nguồn dữ liệu lịch sử khổng lồ. Các nền tảng phân tích dữ liệu lớn (Big data Analysis Frameworks - BDAFs) đã phát triển tương đối mạnh mẽ, nhưng việc áp dụng các nền tảng và kỹ thuật phân tích dữ liệu lớn cho lĩnh vực phân tích và giám sát lưu lượng mạng vẫn chưa được định hình rõ ràng và chuẩn hóa.

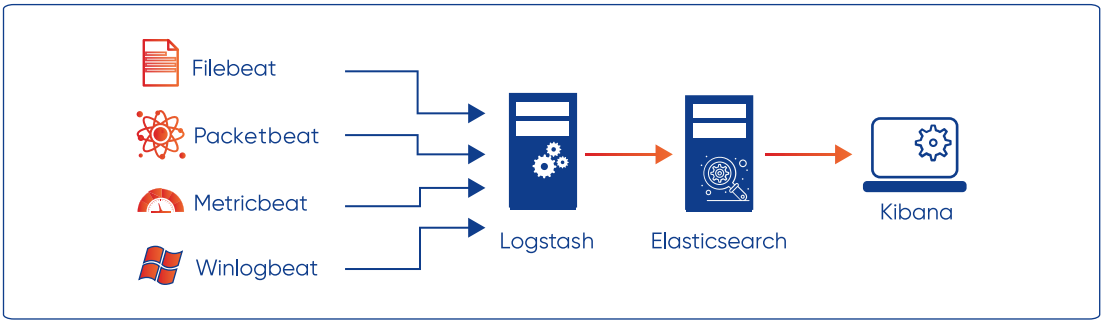
Các cuộc tấn công mạng có chủ đích đã ngày càng trở nên nghiêm trọng và đã trở thành mối đe dọa về an ninh quốc gia. Với công nghệ của tội phạm mạng hiện tại, các cuộc tấn công không chỉ xuất phát từ mạng bên ngoài của các hệ thống CNTT mà còn xuất phát ngay từ trong mạng nội bộ bên trong. Tuy nhiên, các giải pháp phát hiện và chống tấn công mạng hiện tại như Firewall, IDS/IPS, ... đang bị giới hạn chỉ phát hiện và ngăn chặn được các cuộc tấn công từ bên ngoài do sử dụng phương pháp phát hiện tấn công mạng để theo dõi lưu lượng truy cập từ bên ngoài vào bên trong. Do đó việc áp dụng công nghệ Big Data vào thu thập, phân tích các nhật ký hệ thống và thiết bị CNTT trọng yếu giúp tăng cường hơn cho việc đảm bảo an toàn an ninh cho hệ thống.

Dữ liệu được tạo ra bởi các thiết bị, hệ thống CNTT, đặc biệt là các hệ thống đảm bảo an toàn an ninh là rất lớn và đa dạng, do đó yêu cầu công nghệ thu thập và xử lý phải có hiệu năng, tính ổn định và sẵn sàng cao cũng như hỗ trợ cho cả các dữ liệu có cấu trúc và phi cấu trúc. Mô hình thu thập dữ liệu dưới đây được đề xuất để đảm bảo các yêu cầu đó. Mô hình này hỗ trợ hai phương pháp, sử dụng agent và không sử dụng agent để thu thập thông tin. Với các giải pháp, nền tảng thu thập, phaah tích điển hình như sau:

(1) Elastic Stack:

Công cụ mã nguồn mở ELK Stack (Elasticsearch – Logstash – Kibana), hiện tại đã đổi tên thành Elastic Stack, sử dụng để phân tích thời gian thực đối với các nguồn dữ liệu có cấu trúc (structured) cho đến không có cấu trúc (unstructured). Như tên gọi trước đây, bộ công cụ ELK bao gồm 03 thành phần:

- Logstash: dùng để thu thập, xử lý log và chuyển vào lưu trữ trong Elastic Search.
- Elasticsearch: thực hiện đánh chỉ mục, lưu trữ và truy xuất dữ liệu.
- Kibana: là một công cụ Web, cung cấp các giao diện để truy vấn dữ liệu trong Elasticsearch, tạo ra các thành phần hiển thị dữ liệu (widget) như biểu đồ, bảng, ... Các thành phần hiển thị dữ liệu này có thể được nhóm với nhau tạo thành các dashboard sử dụng để giám sát, thống kê dữ liệu.



Hình 50: Mô hình chức năng của các thành phần trong công cụ ELK

Một số tính năng của Elastic Stack:

- Có khả năng thu thập và phân loại được nhiều loại log: web log, system log, application log, device log,...
- Có khả năng xử lý và phân loại log như: windows event log, networking logs, firewall logs, ...
- Khả năng nhận log từ các client thông qua các shipper là các beat platform hoặc syslogng
- Giám sát thời gian gần thực (RealTime - NRT): Elasticsearch là một platform tìm kiếm thời gian gần thực. Có độ trễ nhỏ (độ trễ vài giây) kể từ thời điểm index data đến khi nó có thể phục vụ tìm kiếm.
- Có khả năng mở rộng tốt: hỗ trợ triển khai theo mô hình Cluster. Người dùng có thể triển khai hệ thống ban đầu nhỏ gọn, sau đó mở rộng năng lực hệ thống bằng việc tăng số lượng node trong cluster. Việc thêm các node vào Elasticsearch cluster là tương đối dễ dàng.
- Hỗ trợ kết nối với Bigdata (Hadoop): để lưu trữ và truy cập nhanh chóng các dữ liệu đã được index của ELK trong thời gian dài.
- Hỗ trợ tìm kiếm toàn văn (Full-Text search): Do Elasticsearch được xây dựng trên Apache Lucene là một công nghệ phân tích và tìm kiếm Full-Text rất mạnh.

Một số công cụ để thu thập dữ liệu trong Elastichsearch (được gọi là Beat) chính sau:

- Filebeat: Filebeat là một Beat được sử dụng để thu thập và chuyển dữ liệu từ các tập tin log. Nó theo dõi các tập tin log và gửi các sự kiện log đến Logstash hoặc Elasticsearch để xử lý và lưu trữ.
- Metricbeat: Metricbeat được sử dụng để thu thập thông tin về các chỉ số hệ thống và dịch vụ từ các máy chủ và hệ thống. Nó có thể thu thập các chỉ số CPU, bộ nhớ, tải hệ thống, thông tin về dịch vụ như MySQL, Apache và nhiều hơn nữa. Metricbeat gửi các dữ liệu thu thập được đến Logstash hoặc Elasticsearch để phân tích và hiển thị.
- Packetbeat: Packetbeat là một Beat được sử dụng để thu thập thông tin về giao thức mạng từ dữ liệu gói tin. Nó có thể phân tích và hiểu được các giao thức như HTTP, DNS, ICMP, MySQL, PostgreSQL và nhiều giao thức khác. Packetbeat gửi dữ liệu thu thập được đến Logstash hoặc Elasticsearch để phân tích và xem xét chi tiết về hoạt động mạng.
- Auditbeat: Auditbeat là một Beat được sử dụng để thu thập các sự kiện hệ thống và log kiểm tra an ninh từ các hệ điều hành Linux. Nó có thể thu thập thông tin về hoạt động hệ thống như các sự kiện đăng nhập, thay đổi quyền truy cập file, các sự kiện quản lý quyền truy cập và nhiều hơn nữa. Auditbeat gửi dữ liệu thu thập được đến Logstash hoặc Elasticsearch để phân tích và giám sát an ninh hệ thống.
- Heartbeat: Heartbeat là một Beat được sử dụng để theo dõi sự hoạt động và sự sống còn của các dịch vụ và máy chủ. Nó có thể kiểm tra kết nối mạng, kiểm tra tính khả dụng của dịch vụ web và nhiều kiểm tra khác. Heartbeat gửi thông tin về trạng thái hoạt động đến Logstash hoặc Elasticsearch để giám sát và thông báo sự cố.

Đối với việc phân tích dữ liệu DNS dựa vào phân tích lưu lượng mạng (cụ thể là lưu lượng truy vấn/phản hồi truy vấn DNS), Elasticsearch sử dụng công cụ thu thập dữ liệu gọi là "packetbeat" để thực hiện thu thập và gửi toàn bộ dữ liệu capture từ các cổng mạng liên quan đến DNS về máy chủ lưu trữ, phân tích dữ liệu tập trung để xử lý.

Packetbeat được đóng gói dưới dạng template, chứa các trường thông tin mẫu, tiêu chuẩn và cơ bản về gói tin DNS. Hệ thống thu thập, phân tích tập trung sẽ dựa vào các trường thông tin cơ bản đó để xử lý và đưa ra các dashboard, báo cáo.

Hình 51: Đồ thị giám sát tổng quan hoạt động DNS sử dụng ELK

Hình 52: Đồ thị giám sát chi tiết hoạt động DNS sử dụng ELK

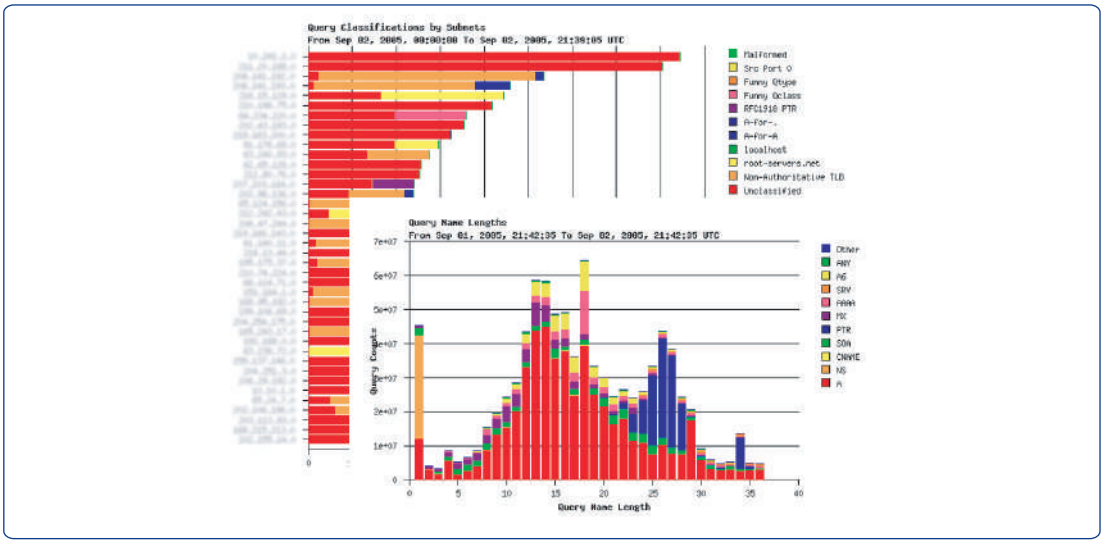
(2) DSC - DNS Statistics Collector:

DNS Statistics Collector (DSC) là phần mềm mã nguồn mở, ban đầu nó được phát triển như một dự án đo lường từ xa cho cộng đồng, bao gồm các thành viên OARC và các tổ chức quản lý vận hành hệ thống máy chủ gốc DNS Root nhằm khuyến khích chia sẻ dữ liệu DNS (gói tin DNS, truy vấn, phản hồi) với nhau để có cái nhìn rõ hơn về DNS và so sánh hệ thống hoạt động như thế nào khi lan truyền trên Internet. Nó vẫn được thiết lập để cho phép người dùng thực hiện việc này, nhưng hiện nay hầu hết các tổ chức đều sử dụng nó để giám sát riêng cho hệ thống DNS.

Nó được thiết kế để sử dụng kiến trúc phân tán với các bộ thu thập chạy trên hoặc "gần" (trong cùng hạ tầng mạng) các máy chủ Authoritative DNS Server, gửi dữ liệu thu thập được đến một hoặc nhiều hệ thống xử lý tập trung để lưu trữ và biểu diện, hiển thị. Công cụ thu thập hay collector sử dụng PCAP để bắt lưu lượng truy cập mạng và truyền dữ liệu tổng hợp đến hệ thống lưu trữ, xử lý và hiển thị gọi chung là presenter dưới dạng dữ liệu XML.

Dữ liệu được thu thập bao gồm:

- Các loại truy vấn
- Mã phản hồi
- Mã lệnh
- Địa chỉ nguồn hoặc mạng con
- Tên truy vấn TLD
- Thông số EDNS
- Các mối đe dọa, tấn công DNS đã biết
- Kích thước bản tin DNS
- IPv4/IPv6
- Cổng TCP/UDP



Hình 53: Đồ thị giám sát hoạt động DNS sử dụng DSC

Hình 54: Đồ thị giám sát hoạt động DNS sử dụng DSC (kết hợp Grafana)

(3) Compacted DNS:

Compacted DNS hay C-DNS là một định dạng lưu trữ dữ liệu DNS được thiết kế để tối ưu hóa kích thước và hiệu suất. Nó dựa trên CBOR (Concise Binary Object Representation), một định dạng mã hóa nhị phân hiệu quả và linh hoạt. C-DNS được đặc tả trong RFC 8618, được tiêu chuẩn hóa vào năm 2019.

Từ lâu, các nhà quản lý vận hành, khai thác hệ thống máy chủ DNS đã có nhu cầu thu thập truy vấn và phản hồi DNS trên các máy chủ Authoritative DNS Server và DNS recursive resolver để theo dõi và phân tích. Dữ liệu này được sử dụng theo một số cách, bao gồm giám sát lưu lượng, phân tích các cuộc tấn công mạng và phân tích "day in the life" (DITL).

Đã có rất nhiều công cụ hỗ trợ việc thu thập dữ liệu lưu lượng DNS như đã đề cập ở trên, chẳng hạn như DNS Statistics Collector (DSC), packetq, dnscap và dnstap.

Tuy nhiên, không có định dạng trao đổi tiêu chuẩn để "chụp" gói tin DNS lớn. Định dạng PCAP ("chụp gói") hoặc định dạng PCAP thế hệ tiếp theo (PCAP-NG) thường được sử dụng trong thực tế để chụp gói, nhưng các định dạng tệp này có thể chứa rất nhiều thông tin bổ sung không phải là liên quan trực tiếp đến phân tích lưu lượng DNS và do đó làm tăng kích thước tệp chụp một cách không cần thiết. Ngoài ra, các công cụ và định dạng này thường không có cơ chế lọc để chỉ ghi có chọn lọc một số trường nhất định tại thời điểm thu thập, yêu cầu xử lý hậu kỳ để ẩn danh hoặc cơ chế mã hóa, bảo mật dữ liệu nhằm bảo vệ quyền riêng tư của người dùng.

Nhiều nhà quản lý, vận hành và khai thác DNS có thể nhận được hàng trăm nghìn truy vấn mỗi giây (qps) trên một máy chủ DNS, do đó, rất mong muốn có một cơ chế giảm thiểu kích thước lưu trữ và truyền tải của dữ liệu được thu thập.

C-DNS (Compacted-DNS), tập trung vào vấn đề thu thập và lưu trữ các tệp chụp gói tin lớn của lưu lượng DNS với các mục tiêu sau:

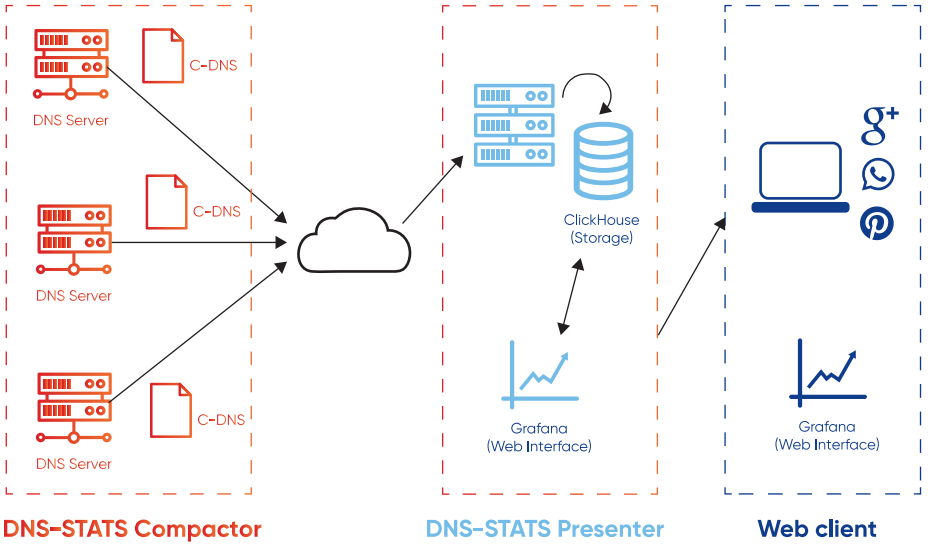
- Giảm thiểu kích thước tệp để lưu trữ và truyền tải.
- Giảm thiểu thời gian tạo và nén các tệp.

Hiện nay, C-DNS được ICANN sử dụng để triển khai cho hệ thống thu thập, giám sát lưu lượng truy cập DNS cho hệ thống DNS Root với tên gọi là DNS-STATS (DNS-STATS Compactor). Giải pháp này được sử dụng để thay thế cho hệ hống sử dụng DSC (DSC sử dụng PCAP để chụp/bắt các gói tin DNS, tuy nhiên PCAP tạo ra các file có kích thước rất lớn, đồng thời việc thực thi PCAP gây ảnh hưởng một phần không nhỏ đến hiệu năng của máy chủ DNS).

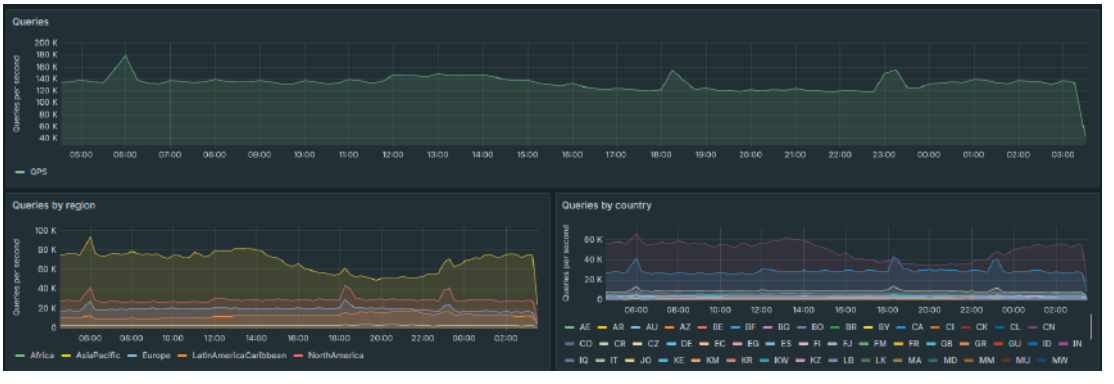
Dự án DNS-STATS Compactor là một bộ công cụ để thu thập và làm việc với lưu lượng truy cập máy chủ DNS được ghi trong các tệp Compacted-DNS (C-DNS). DNS-STATS Compactor ban đầu được phát triển cho ICANN bởi Sinodun IT.

Bộ DNS-STATS Compactor hiện bao gồm hai chương trình:

- compactor: tương tự với cách sử dụng tcpdump, compactor đọc lưu lượng truy cập từ một hoặc nhiều giao diện mạng và ghi các chi tiết đã chọn vào các tệp đầu ra C-DNS và PCAP. máy nén cũng có thể đọc và chuyển



Hình 55: Mô hình logic triển khai C-DNS



Hình 56: Đồ thị giám sát tổng quan hoạt động DNS sử dụng C-DNS

Do đó, việc khai thác thông tin từ dữ liệu lưu lượng hoạt động truy vấn và phản hồi truy vấn DNS từ đó phân tích hành vi truy cập của người dùng để đảm bảo hoạt động liên tục cho hệ thống DNS cũng như phát hiện và cảnh báo sớm các bất thường và đưa ra các phương án xử lý, đảm bảo an toàn an ninh cho hệ thống hiện tại đang là giải pháp rất hiệu quả để đảm bảo cho sự ổn định mạng Internet.

4.3. Blocking DGA

4.3.1. Giới thiệu

- DGA (Domain Generation Algorithms) hay thuật toán tạo tên miền là một kỹ thuật được sử dụng phổ biến bởi các phần mềm độc hại (malware) nhằm kết nối với các máy chủ điều khiển (Command & Control - C&C). DGA cho phép malware tạo (đăng ký) hàng loạt tên miền một cách tự động, khó dự đoán và thay đổi theo thời gian.
- DGA thường được chia thành 2 loại dựa trên đặc điểm tên miền được tạo ra, bao gồm: tên miền giả ngẫu nhiên (pseudo-random) hoặc tên miền dựa trên "từ điển" (ditionary-based).
- Tên miền giả ngẫu nhiên là tên miền được tạo ra bằng kỹ thuật tạo ngẫu nhiên chuỗi ký tự, nó tương tự như việc một người gõ ngẫu nhiên một chuỗi ký tự trên bàn phím, các tên miền này thường là các chuỗi ký tự không có nghĩa, ví dụ: cuxrbykwokrqcldyjawc.com và enjvatxpymxbccdidbmc.com

- Các tên miền dựa trên từ điển thường được tạo bằng cách kết hợp hai hoặc ba từ hoặc một nhóm từ có nghĩa (được lấy trong từ điển) để tạo ra các tên miền trông hợp lý và có thể được tạo bởi con người, thay vì các chuỗi ký tự ngẫu nhiên vô nghĩa. Ví dụ, tên miền được tạo ra bằng cách lấy một từ (là tính từ) trong từ điển như "happy", "sad" và "lovely"; từ thứ hai có thể chứa các danh từ như "shoes", "car" và "ring". Khi kết hợp lại, chúng tạo ra các tên miền như happycars.com hoặc sadshoes.net, trông giống như các tên miền bình thường và được tạo (đăng ký) bởi con người.

Do đó, kẻ tấn công thường sử dụng kỹ thuật DGA này để tạo ngẫu nhiên hàng loạt các tên miền, nhằm sử dụng cho các cuộc tấn công mạng, với số lượng lớn các tên miền trên Internet làm cho việc phát hiện và chặn trở nên rất khó khăn và phức tạp hơn. Loại hình tấn công này khiến việc truy vết và ngăn chặn trở nên khó khăn hơn rất nhiều. Ngay cả khi đã phát hiện và chặn các tên miền và địa chỉ IP được sử dụng trong một ngày, ngày hôm sau lại phải bắt đầu lại từ đầu. Với DGA, kẻ tấn công có lợi thế lớn: chúng biết chính xác hàng nghìn tên miền nào sẽ hoạt động tại bất kỳ thời điểm nào, trong khi người phòng thủ hoàn toàn bị đặt vào thế bị động.

4.3.2. Chặn DGA (Blocking DGA)

Đã có nhiều giải pháp được đưa ra để ngăn chặn DGA, trong đó có cả công nghệ RPZ (Response Policy Zone) đã nêu ở phần trên. Tuy nhiên, RPZ chỉ là một danh sách chặn có khả năng cập nhật tự động, có nghĩa là máy chủ DNS phân giải đệ quy cần lưu trữ danh sách chặn này trong bộ nhớ và so sánh từng truy vấn được gửi đến với danh sách đó.

Khi danh sách chỉ có ít tên miền thì việc kiểm tra một truy vấn tên miền không gây ra bất kỳ ảnh hưởng đáng kể nào. Tuy nhiên, nếu danh sách các tên miền độc hại tăng lên hàng nghìn, việc kiểm tra này có thể gây ra sự chậm trễ nghiêm trọng.

Ví dụ: mã độc Conficker, nó đã trở thành một trong những mã độc lây lan rộng nhất trong lịch sử công nghệ thông tin, ảnh hưởng đến hàng triệu máy tính trên toàn cầu. Điểm khác biệt của Conficker so với các phần mềm độc hại khác nằm ở số lượng tên miền khổng lồ mà nó và các biến thể của nó tạo ra bằng cách sử dụng các thuật toán tạo tên miền (DGA). Các phiên bản ban đầu của Conficker tạo ra 250 tên miền, trong khi các biến thể sau đó có thể tạo ra đến 50.000 tên miền. Các thiết bị bị nhiễm sẽ tìm kiếm các tên miền này và liên lạc với máy chủ điều khiển (C2) thông qua giao thức HTTP/S.

Trong một số các nghiên cứu[8] cho thấy chỉ một phần nhỏ trong số lượng lớn các tên miền do Conficker đăng ký vẫn đang được sử dụng. Tuy nhiên, không thể biết chính xác bao nhiêu trong số đó là không hoạt động và có thể hoạt động trở lại theo lệnh của kẻ tấn công. Như trong trường hợp của Conficker, chỉ một phần mềm độc hại có thể sử dụng hàng chục ngàn tên miền. Việc xác định tất cả những tên miền này là một thách thức lớn, và việc tải một danh sách chặn khổng lồ lên một máy chủ DNS có thể gây ra tải trọng rất lớn.

Nếu tải toàn bộ danh sách tên miền của Conficker vào máy chủ DNS phân giải đệ quy (DNS recursive resolver), danh sách này có thể lên đến hàng triệu tên miền. Điều đó đồng nghĩa với việc cần tải danh sách này vào bộ nhớ của máy chủ DNS và mọi truy vấn ra ngoài phải được kiểm tra so với hàng triệu tên miền đó. Việc này có thể gây ra độ trễ lớn trong hiệu suất DNS, dẫn đến vấn đề hiệu suất mạng tổng thể.

Do đó, cần các phương pháp mới trong việc phát hiện và ngăn chặn tạo tên miền bằng kỹ thuật DGA. Các giải pháp này được gọi là giám sát và phát hiện sớm các dấu hiệu bất thường của tên miền, như giám sát các tên miền mới được đăng ký (NRDs - Newly Registered Domains) dựa vào các thông tin, đặc điểm liên quan đến tên miền: chuỗi ký tự đặc trưng của tên miền (như độ dài bất thường, chuỗi ngẫu nhiên không có nghĩa,...). Hay sử dụng trí tuệ nhân tạo và học máy (AI & ML) để ứng dụng trong việc phân tích và phát hiện bất thường dựa vào lưu lượng DNS (nhiều truy vấn NXDOMAIN, tần suất truy vấn cao, truy vấn đến nhiều miền ngẫu nhiên từ cùng một nguồn, ...) giúp ngăn chặn kịp thời các truy vấn đến tên miền độc hại.

4.4. Mã hóa DNS

Sự phát triển về mã hóa trong lĩnh vực DNS đã diễn ra rất nhanh trong những năm gần đây, và chắc chắn sẽ có nhiều tiến bộ hơn nữa trong tương lai. Trong phần này, chúng tôi cung cấp cái nhìn tổng quan về các khái niệm, giúp các chuyên gia quản lý, vận hành và phát triển hệ thống DNS đưa ra quyết định khi áp dụng các công nghệ đang phát triển này vào thiết kế hệ thống.

Trong các phần trước, chúng tôi đã trình bày các kỹ thuật phát hiện tấn công dựa trên DNS. Những phương pháp này chủ yếu dựa vào khả năng kiểm tra các truy vấn DNS để tìm dấu hiệu của các hoạt động độc hại. Tuy nhiên, với sự xuất hiện của mã hóa DNS, thì nó không còn phù hợp và có thể khiến các hệ thống DNS dễ bị khai thác tấn công bởi các mối đe dọa DNS. Điều đáng lo ngại hơn là nhiều người dùng trên mạng có thể đã và đang sử dụng DNS được mã hóa, vì nó hiện đang được triển khai mặc định trên nhiều trình duyệt. Mặc dù mục đích ban đầu của DNS được mã hóa là để tăng cường tính riêng tư, nhưng một số cách triển khai lại vô tình tạo ra các rủi ro bảo mật nghiêm trọng.

[8] https://circleid.com/posts/20210831-what-are-the-internet-domains-connected-to-the-conficker-botnet

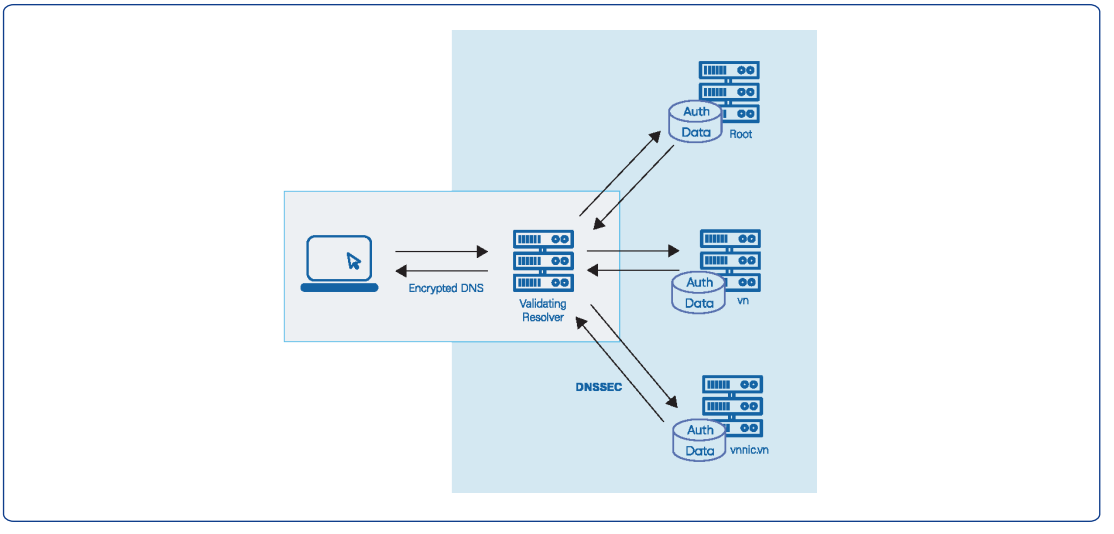
4.4.1. DNS được mã hóa bảo vệ người dùng cuối

DNS được mã hóa là giải pháp hiệu quả trong lĩnh vực DNS nhằm giải quyết vấn đề lạm dụng DNS và bảo vệ quyền riêng tư một cách có hệ thống. Công nghệ này được các nhà cung cấp, phát triển trình duyệt web và người dùng ủng hộ mạnh mẽ. Tuy nhiên, nó không thể bảo vệ trước các cuộc tấn công làm nhiễm độc bộ nhớ đệm (cache poisoning).

Mặc dù DNSSEC đã được triển khai cho zone tên miền, hệ thống máy chủ DNS. Tuy nhiên, phần kết nối giữa hệ thống DNS phân giải xác thực (DNS validating resolver) và thiết bị người dùng cuối (stub resolver) vẫn có nguy cơ bị tấn công. Phần chưa được bảo vệ này còn được gọi là "vấn đề tuyến cuối của DNS" (DNS last-mile problem). Điều cốt lõi của vấn đề này là ngay cả khi khách hàng chỉ truy cập các tên miền đã ký DNSSEC (hiện tại số lượng còn khá ít), và bộ phân giải xác thực kiểm tra từng phản hồi DNS, thì dữ liệu cuối cùng vẫn được gửi đến khách hàng dưới dạng văn bản rõ ràng (clear text), không có bất kỳ hình thức bảo mật mã hóa dữ liệu nào.

Như minh họa dưới đây, một kẻ tấn công có thể đứng giữa người dùng cuối (client) và bộ phân giải xác thực, từ đó theo dõi và thực hiện các cuộc tấn công kiểu man-in-the-middle.

Chúng ta có thể bảo vệ tuyến cuối này bằng mã hóa DNS. Tuy nhiên, cần lưu ý rằng giải pháp này chỉ mã hóa dữ liệu truyền tải giữa client và bộ phân giải được cấu hình. Nó không cung cấp mã hóa toàn diện cho toàn bộ quá trình phân giải DNS – tức là, truyền tải giữa các máy chủ DNS vẫn không được mã hóa.



Hình 57: Mã hóa DNS

4.4.2. Các tiêu chuẩn mã hóa DNS phổ biến hiện nay

Về bản chất, mã hóa DNS sử dụng mã hóa để bảo vệ các bản tin DNS khỏi sự theo dõi, bao gồm cả những kẻ tấn công và các công ty muốn thu thập và thương mại hóa từ dữ liệu người dùng mà không có sự cho phép.

Mã hóa khóa công khai, đặc biệt là giao thức bảo mật lớp truyền tải (TLS - Transport Layer Security). TLS đã được sử dụng rộng rãi trong việc bảo vệ hầu hết các giao tiếp trên Internet, bao gồm HTTPS, đảm bảo tính bảo mật và tính toàn vẹn của dữ liệu. Tuy nhiên, việc áp dụng TLS vào hệ thống DNS cũng đặt ra những thách thức riêng:

- Một vấn đề quan trọng khi triển khai DNS được mã hóa là yêu cầu sử dụng giao thức TCP thay vì UDP.
- Hầu hết các giao thức DNS truyền thống hoạt động trên UDP (User Datagram Protocol), vì nó cho phép truy vấn nhanh chóng và hiệu quả, với độ trễ thấp.
- Ngược lại, TLS cần chạy trên TCP (Transmission Control Protocol), vốn có cơ chế xác nhận gói tin và bảo mật tốt hơn, nhưng lại làm tăng độ trễ do cần thêm bước thiết lập kết nối (TCP handshake) và cơ chế mã hóa dữ liệu.

Việc thay đổi từ UDP sang TCP có thể gây ra những ảnh hưởng đáng kể đến hiệu suất của hệ thống DNS, đặc biệt khi xét đến khối lượng truy vấn khổng lồ mà DNS phải xử lý hàng ngày. Điều này là một trong những nguyên nhân chính khiến việc triển khai DNS được mã hóa diễn ra chậm hơn so với các công nghệ mã hóa khác trên Internet.

Trong nhiều năm qua, cộng đồng DNS ngày càng nhận thức rõ hơn về mối quan ngại đối với quyền riêng tư khi sử dụng DNS truyền thống. Các truy vấn DNS gửi dưới dạng văn bản rõ ràng (clear text) có thể bị chặn, giám sát, nghe lén hoặc thậm chí bị chỉnh sửa bởi các bên trung gian như nhà cung cấp dịch vụ Internet (ISP), chính phủ hoặc các tổ chức thu thập, giám sát.

Chính vì vậy, nhiều phương pháp đã được đề xuất để thêm hỗ trợ mã hóa vào hệ thống DNS, với mục tiêu bảo vệ người dùng khỏi các nguy cơ rò rỉ thông tin truy vấn DNS.

Một số tiêu chuẩn mã hóa DNS đã được phát triển và triển khai rộng rãi, trong đó có hai công nghệ nổi bật nhất hiện nay là:

- DNS over TLS (DoT) - DNS qua giao thức bảo mật lớp truyền tải
- DNS over HTTPS (DoH) - DNS qua giao thức bảo mật HTTPS

Hai công nghệ này có những điểm tương đồng trong việc cung cấp mã hóa cho truy vấn DNS, nhưng cũng có những điểm khác biệt quan trọng trong cách chúng hoạt động và mức độ bảo mật mà chúng mang lại.

Khi thảo luận về DoT và DoH, chúng ta cũng sẽ sử dụng thuật ngữ DNS truyền thống để chỉ DNS hoạt động trên cổng 53 (Do53), thường được gọi tắt là "dose" – một cách diễn giải phổ biến trong giới chuyên môn.

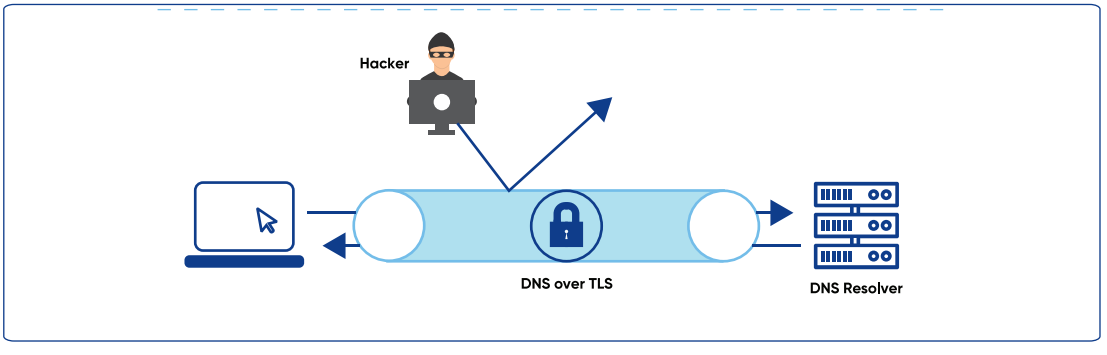
a. DNS Over TLS (DoT) – Bảo mật truy vấn DNS bằng giao thức mã hóa lớp truyền tải

Trong bối cảnh an ninh mạng ngày càng trở thành mối quan tâm hàng đầu, việc bảo vệ truy vấn DNS trước sự theo dõi và tấn công từ bên thứ ba là điều vô cùng quan trọng. DNS Over TLS (DoT) ra đời với mục tiêu chính là mã hóa toàn bộ truy vấn DNS, giúp ngăn chặn các cuộc tấn công man-in-the-middle (MitM), đồng thời đảm bảo quyền riêng tư của người dùng trên Internet.

- Cơ chế hoạt động của DoT

Khác với DNS truyền thống hoạt động dựa trên giao thức UDP trên cổng 53, DoT thực hiện truy vấn DNS thông qua giao thức TCP trên cổng 853, sau đó bổ sung một lớp mã hóa TLS để bảo vệ nội dung truy vấn. Điều này giúp đảm bảo rằng tất cả dữ liệu trao đổi giữa máy khách (client) và máy chủ DNS (resolver) được mã hóa toàn bộ, hạn chế tối đa nguy cơ bị nghe lén hoặc sửa đổi nội dung.

Khi một thiết bị gửi yêu cầu DNS bằng DoT, hệ thống sẽ thực hiện thiết lập kết nối bảo mật (TLS handshake) trước khi truyền tải dữ liệu. Quá trình này có thể gây ra độ trễ cao hơn so với DNS truyền thống, nhưng đổi lại, người dùng sẽ có một môi trường an toàn hơn để thực hiện các truy vấn DNS.



Hình 58: DNS over TLS (DoT)

- Lợi ích của DoT

Một trong những ưu điểm lớn nhất của DoT là khả năng bảo vệ quyền riêng tư bằng cách mã hóa toàn bộ truy vấn DNS. Do đó, nhà cung cấp dịch vụ Internet (ISP), hacker hay bất kỳ bên thứ ba nào cũng không thể theo dõi hoặc can thiệp vào hoạt động DNS của người dùng. Đồng thời, DoT còn giúp ngăn chặn các cuộc tấn công DNS spoofing và DNS cache poisoning, những kỹ thuật tấn công phổ biến nhằm làm sai lệch thông tin phân giải tên miền.

- Những thách thức khi triển khai DoT

Mặc dù mang lại nhiều lợi ích, DoT cũng đối mặt với một số hạn chế nhất định. Việc sử dụng TCP thay vì UDP khiến cho tốc độ phản hồi của DNS có thể chậm hơn, đặc biệt là trong những hệ thống có lượng truy vấn DNS lớn. Hơn nữa, không phải tất cả các nhà cung cấp DNS đều hỗ trợ DoT, và việc triển khai trên diện rộng đòi hỏi sự thay đổi từ cả phía máy khách và máy chủ.

Ngoài ra, vì DoT sử dụng một cổng TCP riêng biệt (853), nó có thể bị chặn dễ dàng bởi các hệ thống tường lửa hoặc nhà cung cấp dịch vụ Internet. Điều này khiến DoT không phải là một lựa chọn lý tưởng trong môi trường có kiểm soát chặt chẽ về lưu lượng mạng.

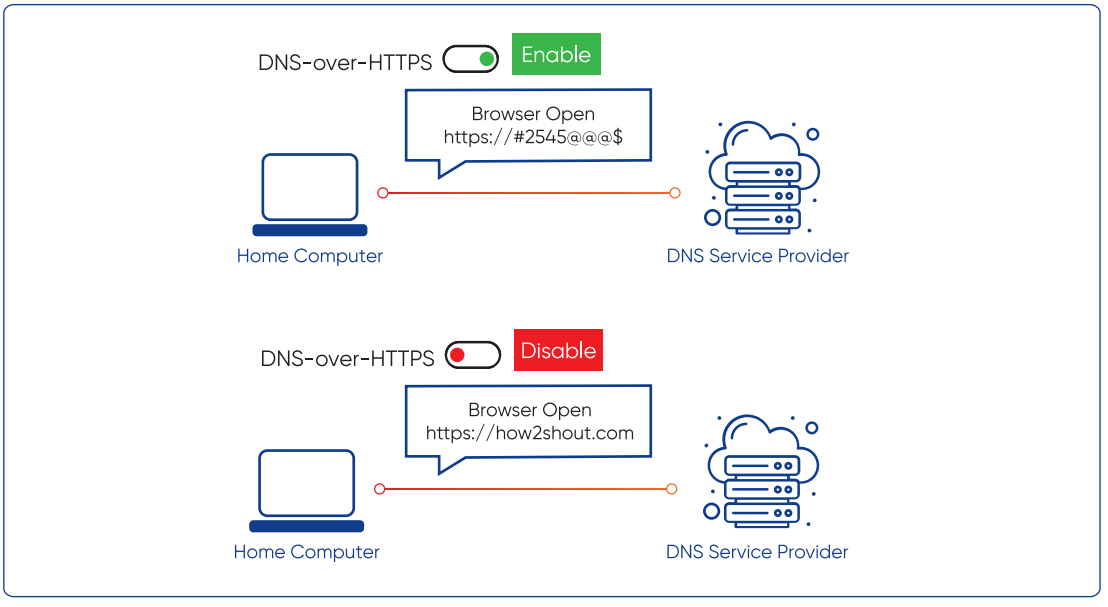
b. DNS Over HTTPS (DoH) – Bảo mật truy vấn DNS thông qua giao thức HTTPS

Nếu như DoT bảo vệ truy vấn DNS bằng cách mã hóa nó qua giao thức TLS trên TCP/853, thì DNS Over HTTPS (DoH) lại thực hiện một cách tiếp cận hoàn toàn khác: ẩn giấu truy vấn DNS trong lưu lượng HTTPS thông thường.

- Nguyên lý hoạt động của DoH

DoH hoạt động bằng cách mã hóa truy vấn DNS và truyền nó thông qua giao thức HTTPS (cổng 443) – cổng mặc định mà tất cả các trình duyệt web và ứng dụng Internet sử dụng để giao tiếp với các trang web an toàn. Điều này có nghĩa là truy vấn DNS khi sử dụng DoH sẽ giống như bất kỳ lưu lượng HTTPS nào khác, giúp chúng tránh bị phát hiện hoặc chặn bởi các nhà cung cấp dịch vụ hoặc hệ thống tường lửa.

Một điểm đặc biệt của DoH là nó có thể được triển khai trực tiếp trên trình duyệt web. Các trình duyệt như Google Chrome, Mozilla Firefox, Microsoft Edge đều đã hỗ trợ DoH, cho phép người dùng tự động chuyển đổi sang DoH mà không cần thay đổi cấu hình của hệ thống.



Hình 59: DNS over HTTPS (DoH)

- Lợi ích vượt trội của DoH

Nhờ khả năng "ẩn" trong lưu lượng HTTPS, DoH mang lại mức độ bảo mật và quyền riêng tư cao hơn đáng kể so với DoT. Khi sử dụng DoH, truy vấn DNS của người dùng sẽ không thể bị ISP theo dõi, chặn hoặc sửa đổi, giúp người dùng bypass (vượt qua) các hạn chế DNS do nhà cung cấp dịch vụ áp đặt các chính sách tường lửa.

Ngoài ra, DoH cũng phù hợp với những người dùng thường xuyên di chuyển, vì họ có thể sử dụng DoH trên các thiết bị cá nhân mà không cần cấu hình lại hệ thống mạng. Hiện nay có các dịch vụ DoH công khai như Google (8.8.8.8), Cloudflare (1.1.1.1) hoặc Quad9 (9.9.9.9), ...

- Những thách thức và rủi ro khi sử dụng DoH

Tuy nhiên, chính vì khả năng ẩn danh quá tốt, DoH cũng đặt ra nhiều thách thức cho quản trị hệ thống mạng và các chuyên gia bảo mật. Vì các truy vấn DNS được mã hóa và giấu trong HTTPS, các hệ thống giám sát mạng truyền thống không thể theo dõi hoặc kiểm soát hoạt động DNS. Điều này gây ra khó khăn trong việc phát hiện và ngăn chặn các mối đe dọa bảo mật, đặc biệt là trong các môi trường doanh nghiệp.

Một trong những rủi ro lớn nhất là tin tặc có thể lợi dụng DoH để che giấu hoạt động độc hại. Các công cụ tấn công mạng như CobaltStrike, Silver đã tích hợp DoH để thực hiện các chiến dịch xâm nhập, khiến việc phát hiện và ngăn chặn trở nên vô cùng khó khăn.

Bên cạnh đó, không giống như DoT, DoH không hỗ trợ cơ chế mã hóa cơ hội (Opportunistic Encryption). Điều này có nghĩa là nếu máy chủ DoH không khả dụng, hệ thống sẽ quay lại sử dụng DNS không mã hóa (Do53) mà không có cơ chế bảo vệ, tạo ra một lỗ hổng bảo mật tiềm tàng.

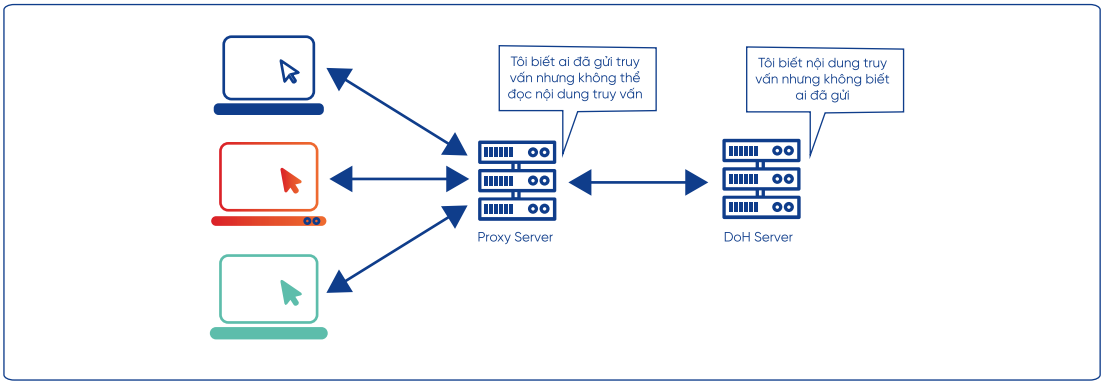
- Giải pháp nâng cao: Oblivious DoH (ODoH)

Trước những lo ngại về quyền riêng tư, Oblivious DoH (ODoH) đã được phát triển để cải thiện DoH bằng cách giấu cả địa chỉ IP của người dùng khi gửi truy vấn DNS.

ODoH hoạt động bằng cách sử dụng một proxy trung gian để tách biệt danh tính của người dùng với nội dung truy vấn DNS. Cụ thể:

- Proxy biết ai đã gửi truy vấn nhưng không thể đọc nội dung truy vấn
- Máy chủ DoH biết nội dung truy vấn nhưng không biết ai đã gửi

Điều này giúp đảm bảo tính ẩn danh hoàn toàn, nhưng cũng đặt ra thách thức về hiệu suất và độ tin cậy, do việc sử dụng proxy có thể làm chậm tốc độ phản hồi DNS.



Hình 60: Oblivious DoH (ODoH)

Các công nghệ mã hóa DNS không chỉ mang lại quyền riêng tư cao hơn mà còn tăng cường khả năng kiểm soát của người dùng đối với hệ thống DNS. Đa số các triển khai mã hóa DNS cho phép người dùng ghi đè cài đặt DNS mặc định của hệ điều hành, trong khi một số giải pháp còn cung cấp cơ chế kiểm soát chi tiết hơn, chẳng hạn như điều chỉnh theo từng ứng dụng hoặc theo từng tên miền cụ thể. Tuy nhiên, tùy vào cách thức triển khai, mức độ kiểm soát lớn hơn có thể tạo ra cảm giác sai lầm về quyền riêng tư, đồng thời làm cho các doanh nghiệp khó thực thi các chính sách bảo mật DNS của họ. Ví dụ dưới đây để làm rõ vấn đề này.

Người dùng A là một người dùng có ý thức về bảo mật. Sau khi tìm hiểu về DNS mã hóa, đã quyết định bật DNS over HTTPS (DoH) trên điện thoại Android và sử dụng máy chủ DoH công cộng của Google. Điều này đồng nghĩa với việc tất cả lưu lượng DNS của A sẽ được mã hóa và gửi đi qua TCP cổng 443 đến máy chủ DoH công cộng của Google (8.8.8.8). Bên cạnh đó, A còn tinh chỉnh cài đặt trên trình duyệt Firefox để mọi truy vấn DNS từ trình duyệt này sẽ được gửi đến máy chủ DoH của Cloudflare (1.1.1.1). Thậm chí, A còn thiết lập một quy tắc đặc biệt để mọi truy vấn đến tên miền vnnic.vn sẽ sử dụng máy chủ DoH của Quad9 (9.9.9.9).

Với các điều chỉnh này, A cảm thấy tự tin rằng mình đã kiểm soát hoàn toàn quyền riêng tư DNS, tin rằng nhà cung cấp dịch vụ Internet (ISP) của anh không thể theo dõi hoặc bán dữ liệu DNS của anh cho bên thứ ba. Nhưng liệu điều đó có thực sự đúng?

Từ góc nhìn của quản trị hệ thống, sự riêng tư mà A nghĩ rằng mình đạt được không thực sự chính xác. Mặc dù các truy vấn DNS của A không còn hiển thị với ISP, nhưng thay vào đó chúng lại chuyển đến các công ty lớn như Google, Cloudflare và Quad9. Những tổ chức này có thể đang thực hiện phân tích dữ liệu DNS của người dùng, thậm chí có thể kiếm lợi từ việc bán dữ liệu hoặc tối ưu hóa quảng cáo, điều mà ISP của Nam trước đây không làm.

Cấu hình này có thể hoạt động tốt tại nhà của A, nhưng khi đến nơi làm việc và kết nối vào mạng nội bộ của công ty, hệ thống có thể gặp sự cố khi không thể truy vấn các tên miền nội bộ, chẳng hạn như ldap.company.local. Ngoài ra, việc thiết lập DNS phức tạp trên thiết bị di động cũng có thể gây khó khăn khi khắc phục sự cố. Đặc biệt, vì mọi lưu lượng DNS của A đều được mã hóa, đội bảo mật tại công ty không thể giám sát hoạt động truy vấn DNS của A, không thể áp dụng hoặc thực thi bất kỳ chính sách bảo mật DNS nào.

Bên cạnh đó, mã hóa DNS cũng mang lại lợi ích cho những kẻ tấn công. Việc mã hóa lưu lượng DNS giúp che giấu hoạt động độc hại, khiến việc giám sát trở nên khó khăn hơn. Như vậy, mã hóa DNS có thể vô tình trở thành một lớp bảo vệ bổ sung cho tội phạm mạng, điều này sẽ được đề cập chi tiết hơn trong các nghiên cứu điển hình sau.

Dịch vụ DNS mã hóa công khai (Public Encrypted DNS) ngày càng thu hút sự chú ý, đặc biệt do tính dễ cài đặt đối với người dùng cuối. Kể từ năm 2020, các trình duyệt như Firefox và Chrome đã bật sẵn DoH theo mặc định. Các hệ điều hành di động như iOS và Android cũng đã hỗ trợ DoH và DoT một cách tự nhiên. Ngay cả Microsoft cũng đã thêm hỗ trợ DoH vào các hệ điều hành của mình như Windows 10 và Windows Server 2022. Những triển khai mặc định này có nghĩa là nhiều người dùng hiện đang sử dụng DoH mà không hề nhận ra, vì trình duyệt của họ tự động gửi truy vấn DNS đến các nhà cung cấp DoH công cộng.

Điều này đặt ra câu hỏi: các nhà cung cấp dịch vụ DNS công khai xử lý dữ liệu quyền riêng tư của người dùng như thế nào? Để làm rõ vấn đề, chúng ta có thể so sánh các chính sách quyền riêng tư của các nhà cung cấp dịch vụ DNS mã hóa phổ biến như sau:

- Google Public DNS: Là một trong những dịch vụ phổ biến nhất, Google Public DNS đã trở thành tiêu chuẩn mà ngay cả những người không có chuyên môn kỹ thuật cũng biết cách sử dụng địa chỉ IP 8.8.8.8 để phân giải DNS. Vào tháng 6 năm 2019, Google công bố hỗ trợ DoH. Theo chính sách quyền riêng tư của họ, Google không thu thập thông tin cá nhân từ người dùng DNS Public, cũng như không sử dụng nó để nhắm mục tiêu quảng cáo. Tuy nhiên, Google vẫn lưu giữ hai loại nhật ký: tạm thời và vĩnh viễn. Nhật ký tạm thời chứa địa chỉ IP nguồn của truy vấn và sẽ bị xóa tự động sau 48 giờ. Nhật ký vĩnh viễn thay thế địa chỉ IP nguồn bằng vị trí thành phố hoặc vùng và giữ lại các thông tin hệ thống như ECS (EDNS Client Subnet) và AS (Autonomous System).
- Cloudflare DNS (1.1.1.1): Nếu tải xuống Firefox ở khu vực Bắc Mỹ, đây sẽ là một trong những nhà cung cấp DNS mặc định trong trình duyệt. Cloudflare cung cấp DoH công khai trên địa chỉ IP 1.1.1.1, với nhiều cấp độ dịch vụ từ miễn phí cho người dùng cá nhân đến các gói trả phí dành cho doanh nghiệp. Theo chính sách quyền riêng tư của Cloudflare, họ không thu thập thông tin cá nhân từ truy vấn DNS và chỉ lưu giữ một phần địa chỉ IP. Phần lớn dữ liệu DNS được lưu trữ trong 24 giờ, sau đó được chia sẻ với APNIC để nghiên cứu.
- Cisco (Umbrella/OpenDNS): Cisco sở hữu dịch vụ OpenDNS, hiện là một phần của danh mục Umbrella. Giống như Cloudflare, OpenDNS cung cấp nhiều cấp độ dịch vụ khác nhau. Tuy nhiên, phiên bản miễn phí yêu cầu người dùng đăng ký tài khoản. Chính sách quyền riêng tư của Cisco không nói rõ họ theo dõi hoặc lưu trữ thông tin gì, nhưng theo Umbrella Privacy Data Sheet, họ thu thập dữ liệu cá nhân, bao gồm cả thông tin Active Directory của tổ chức. Cisco sử dụng dữ liệu này để dự đoán các mối đe dọa và nâng cao thông tin tình báo an ninh mạng cho khách hàng.
- Quad9 (9.9.9.9): Quad9 là một tổ chức phi lợi nhuận, có trụ sở tại Thụy Sĩ và chịu sự điều chỉnh bởi các luật bảo vệ dữ liệu của Châu Âu, như GDPR. Ngoài việc cung cấp dịch vụ DNS mã hóa miễn phí như DoH và DoT, Quad9 còn lọc các miền độc hại mà không tính phí người dùng, trong khi nhiều nhà cung cấp khác chỉ cung cấp dịch vụ này dưới dạng trả phí. Quad9 không lưu giữ địa chỉ IP của người dùng nhưng thu thập dữ liệu dựa trên quốc gia, khu vực và số hiệu mạng (ASN). Dữ liệu này sau đó được chia sẻ với một nhóm nhỏ các chuyên gia bảo mật để nghiên cứu mối đe dọa.

Do đó, không phải tất cả các nhà cung cấp DNS mã hóa đều được tạo ra như nhau, và không phải tất cả đều cung cấp cùng mức độ bảo vệ quyền riêng tư cho người dùng. Nên khi sử dụng dịch vụ DNS mã hóa công khai, người dùng cần hiểu rõ quyền riêng tư của mình, đọc kỹ chính sách sử dụng và đưa ra quyết định phù hợp.

4.4.3. Lợi ích và rủi ro tiềm ẩn

Việc mã hóa DNS mang lại quyền riêng tư đáng kể cho người dùng, giúp bảo vệ họ khỏi sự giám sát của một số quản trị viên mạng hoặc nhà cung cấp dịch vụ Internet (ISP). Tuy nhiên, chính tính năng bảo vệ này cũng có thể bị lợi dụng bởi những kẻ xấu nhằm che giấu các hoạt động độc hại của chúng. Nếu không có DNS mã hóa, cán bộ quản trị có thể dễ dàng theo dõi các truy vấn DNS, từ đó phát hiện sớm các hành vi đáng ngờ, như truy cập vào các tên miền chứa mã độc hoặc các máy chủ điều khiển (C2). Nhờ khả năng quan sát này, các biện pháp bảo mật mạng có thể bảo vệ người dùng khỏi việc truy cập vào các trang web độc hại.

Tuy nhiên, khi DNS được mã hóa, cán bộ quản trị hệ thống mất đi khả năng giám sát các truy vấn DNS một cách trực tiếp. Điều này đồng nghĩa với việc họ không còn có thể theo dõi hành vi của người dùng hay phát hiện các truy vấn DNS độc hại. Đối với người dùng thông thường, đây có thể là một sự đảm bảo về quyền riêng tư. Nhưng đối với các chuyên gia bảo mật, điều này làm giảm khả năng kiểm soát và quản lý mối đe dọa trên hệ thống mạng.

Hơn nữa, việc DNS mã hóa có thể ngăn cản các việc triển khai, áp dụng các biện pháp bảo vệ truyền thống dựa trên DNS, chẳng hạn như RPZ (Response Policy Zones) – một phương pháp chặn truy cập vào các tên miền độc hại. Điều này có thể tạo ra lỗ hổng mà tin tặc có thể lợi dụng để thực hiện các cuộc tấn công tinh vi hơn, mà không bị phát hiện một cách dễ dàng. Trường hợp nghiên cứu về GodLUA dưới đây là một ví dụ điển hình về cách tin tặc đã tận dụng DNS mã hóa để ẩn danh và duy trì hoạt động độc hại mà không bị phát hiện.

GodLUA – Mã độc tận dụng DNS mã hóa để che giấu hoạt động

GodLUA là một phần mềm độc hại được phát hiện vào năm 2019, chỉ vài tháng sau khi RFC 8484, tiêu chuẩn chính thức của DNS-over-HTTPS (DoH), được phê duyệt. Nhóm nghiên cứu bảo mật NetLabs[9] đã phát hiện rằng GodLUA là một trong những phần mềm độc hại đầu tiên lợi dụng DoH để thực hiện giao tiếp với máy chủ điều khiển (C2), khiến nó gần như không thể bị phát hiện bằng các phương pháp giám sát DNS truyền thống.

[9] https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/

Cách GodLUA sử dụng DNS để duy trì hoạt động:
Ban đầu, các phiên bản đầu tiên của GodLUA vẫn dựa vào truy vấn DNS không mã hóa (unencrypted DNS) để tìm kiếm các máy chủ điều khiển C2. Sau đó, phần mềm độc hại này chuyển sang sử dụng các kênh liên lạc khác, chẳng hạn như HTTPS, để tải xuống các payload độc hại. Những phiên bản sau của GodLUA tiếp tục tiến hóa bằng cách tận dụng bản ghi TXT trong DNS để truyền tải mã độc một cách tinh vi hơn.
Tuy nhiên, điểm đáng chú ý nhất là phiên bản GodLUA mới nhất đã chuyển hoàn toàn sang sử dụng DoH, có nghĩa là tất cả thông tin liên lạc giữa máy bị nhiễm và máy chủ C2 đều được mã hóa trong các gói HTTPS. Điều này làm cho việc giám sát hoặc chặn các hoạt động độc hại của GodLUA trở nên cực kỳ khó khăn đối với các hệ thống bảo mật truyền thống.

Cách tin tặc che giấu dấu vết với DoH:
Nhóm tác giả hoặc nhóm đứng sau GodLUA rất tự tin vào khả năng ẩn danh của DoH, đến mức họ không cần phải tạo các tên miền giả (look-alike domains) hoặc đăng ký tên miền bằng DGA (Domain Generation Algorithm) như cách các phần mềm độc hại thông thường vẫn làm. Thay vào đó, GodLUA[10] sử dụng một tên miền mã hóa cứng (hardcoded domain), chẳng hạn như d.heheda.tk, sau đó mở rộng sang sử dụng cloudappconfig.com như một máy chủ điều khiển.
Kỹ thuật này cho phép GodLUA thực hiện các giao tiếp với máy chủ C2 dưới dạng các tin nhắn DoH được mã hóa hoàn toàn, ẩn mình trong lưu lượng HTTPS hợp pháp. Hậu quả là, các hệ thống giám sát an ninh mạng thông thường không thể phân biệt được lưu lượng hợp pháp và lưu lượng độc hại, khiến nó trở thành một mối đe dọa khó phát hiện.

```
GET /dns-query?name=t.cloudappconfig.com&type=TXT HTTP/1.1
Host: cloudflare-dns.com
Accept: application/dns-json

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 10:22:25 GMT
Content-Type: application/dns-json
Content-Length: 345
Connection: keep-alive
Access-Control-Allow-Origin: *
cache-control: max-age=214
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 4ece75c228ebb120-HKG

{"Status": 0,"TC": false,"RD": true, "RA": true, "AD": false,"CD": false,"Question":[{"name": "t.cloudappconfig.com.", "type": 16}],"Answer":[{"name":
"t.cloudappconfig.com.", "type": 16, "TTL": 214, "data": "\"6TmRMwDwSR/sNSEhjCByEw0Vb44nZhEUyUpUR4LcijfIukjdAv+vqqMuYOFAoOpC7KtyyrGnUOqO9XnDpudVmbGoTeJD6hYrw72YmiOS9dX5M/
sPNmsw/eY/XDYYzx5/\""}]}
```

4.4.4. Giảm thiểu rủi ro từ mã hóa DNS

Do những thay đổi được thực hiện bởi các trình duyệt chính và các nhà cung cấp hệ điều hành, do đó hầu hết các doanh nghiệp sẽ bị buộc phải cung cấp dịch vụ DoT hoặc DoH nội bộ. Việc cho phép người dùng doanh nghiệp kết nối với các máy chủ DNS mã hóa bên ngoài mang lại một rủi ro đáng kể đối với an ninh hệ thống.

Điều này có nghĩa là tổ chức cần có năng lực vận hành và duy trì các máy chủ DoT hoặc DoH nội bộ. Nếu không làm như vậy, doanh nghiệp sẽ mất quyền kiểm soát lưu lượng DNS của mình, vì người dùng sẽ truy vấn đến các máy chủ DNS bên ngoài mà doanh nghiệp không thể kiểm soát. Điều này cũng đồng nghĩa với việc không thể thực thi các chính sách bảo mật để kiểm tra lưu lượng DNS đã mã hóa, khiến các biện pháp an ninh mạng như RPZ trở nên vô dụng. Cho đến khi có hệ thống DNS mã hóa nội bộ, doanh nghiệp có thể thực hiện các biện pháp sau để giảm thiểu rủi ro:

- **Vô hiệu hóa DoT hoặc DoH trên hệ điều hành và phần mềm của người dùng:** Nếu có thể, nên hạn chế hoặc vô hiệu hóa các cài đặt DoT và DoH trên thiết bị khách để ngăn người dùng vô tình kích hoạt chúng. Một số trình duyệt web được thiết lập mặc định với DoH đã được bật.
- **Hạn chế truy cập vào các máy chủ DNS mã hóa bên ngoài:** Chặn hoặc giới hạn quyền truy cập đến các máy chủ DoT và DoH bên ngoài giúp đảm bảo rằng không ai trong mạng doanh nghiệp có thể bỏ qua chính sách bảo mật để kết nối đến các máy chủ DNS độc hại. Việc này dễ dàng thực hiện với DoT bằng cách chặn cổng TCP 853, nhưng DoH lại khó bị ngăn chặn hơn.

DoH được thiết kế để trông giống như các tin nhắn HTTPS thông thường, khiến việc phân biệt giữa một yêu cầu trang web thông thường và một truy vấn DNS trở nên khó khăn. Cách duy nhất để xác định một tin nhắn HTTPS có phải là truy vấn DNS hay không là giải mã lưu lượng và thực hiện kiểm tra chuyên sâu trên tin nhắn.

[10] https://blog.netlab.360.com/content/images/2019/06/dnstxt.PNG

Do TCP cổng 443 là chuẩn mực cho truy cập Internet, chúng ta không thể chặn hoàn toàn cổng này mà chỉ có thể thực hiện các biện pháp hạn chế sau để kiểm soát truy cập DoH:

(1) Sử dụng Proxy: Một số tổ chức có thể sử dụng proxy web truyền thống (hoặc proxy trong suốt) để ép buộc người dùng phải đi qua proxy này. Điều này giúp cho phép kiểm tra và chặn các tin nhắn DoH đã mã hóa.

(2) Chặn các máy chủ DoH công khai: Một cách tiếp cận khác là chặn quyền truy cập HTTPS đến các máy chủ DoH công khai. Ví dụ, nếu người dùng đang cố gắng kết nối đến địa chỉ IP 8.8.8.8 qua cổng 53, chúng ta biết rằng đây là DNS thông thường (Do53). Tuy nhiên, nếu người dùng cố gắng kết nối đến địa chỉ này qua cổng 443, điều đó có nghĩa là đang sử dụng DoH. Trong trường hợp đó, doanh nghiệp nên chặn quyền truy cập này.

Một số nhà cung cấp bảo mật cung cấp danh sách các máy chủ DoH công khai, giúp quản trị viên có thể thêm chúng vào danh sách chặn trên hệ thống an ninh mạng của mình.

(3) Sử dụng Canary Domains: Một phương pháp khác, được Mozilla đề xuất và đã được các nhà cung cấp trình duyệt lớn áp dụng, là sử dụng các "canary domains" (tên miền cảnh báo). Bằng cách thiết lập một tên miền đặc biệt như use-application-dns.net để làm "công tắc tắt" DoH. Khi trình duyệt thực hiện truy vấn DNS đến tên miền này, nếu nhận được phản hồi NXDOMAIN (tên miền không tồn tại), nó sẽ hiểu rằng DoH không được phép sử dụng và tự động quay lại Do53.

XIII

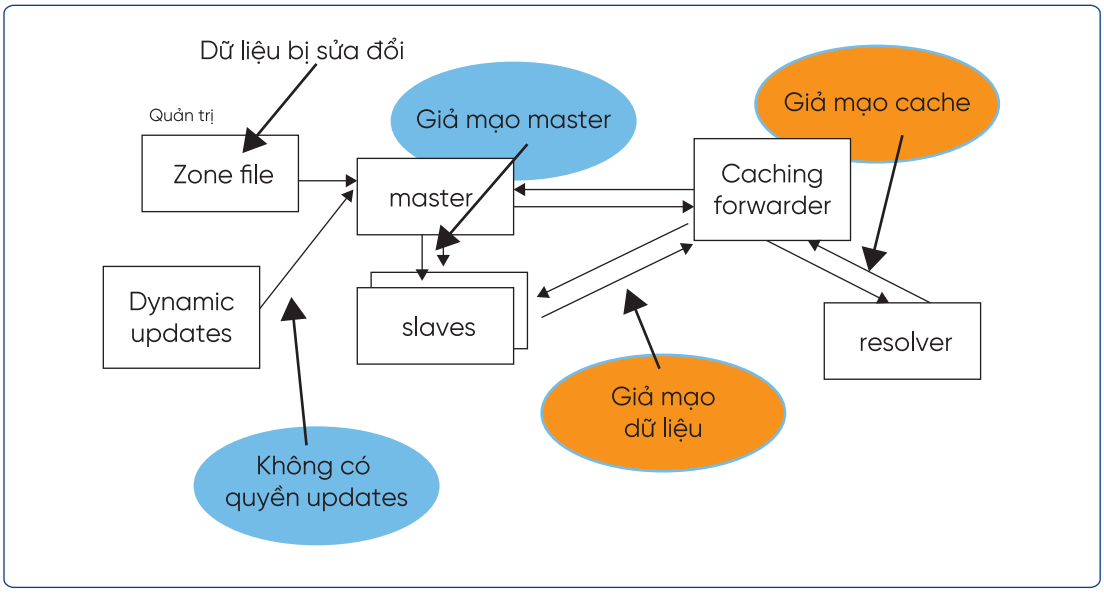
DNSSEC

1. Tổng quan về DNSSEC

1.1. Sự ra đời của DNSSEC

Theo thời gian, hệ thống DNS ngày càng phát triển, đã có hàng trăm triệu tên miền đã được cấp phát, sử dụng để cung cấp các dịch vụ trực tuyến trên Internet. Điều này cũng dẫn đến các hành vi thâm nhập trái phép, chuyển hướng truy cập người dùng, phát tán mã độc, tấn công lạm dụng DNS ngày một nhiều hơn. Các tổ chức nghiên cứu về Internet, các nhà cung cấp thiết bị, dịch vụ đã tập trung nghiên cứu và công bố các tiêu chuẩn về DNS để tăng cường khả năng bảo mật, dự phòng của hệ thống, đồng thời thay đổi, nâng cấp các phiên bản phần mềm DNS để vá lỗi an ninh bảo mật.

Tuy nhiên trong suốt quá trình khai thác, vận hành hệ thống DNS, từ việc cập nhật dữ liệu vào hệ thống cho đến các quá trình tìm kiếm và trả lời thông tin truy vấn từ các trình phân giải tên miền đến các hệ thống DNS đều có thể xảy ra nhiều lỗ hổng về bảo mật mà giao thức DNS thông thường không thể đáp ứng được. Nếu không có hệ thống xác thực, việc cập nhật dữ liệu vào hệ thống sẽ có nguy cơ giả mạo quyền cập nhật thông tin. Quá trình đồng bộ dữ liệu giữa DNS thứ cấp (secondary) và máy chủ DNS chính (primary) có nhiều khả năng sẽ bị giả mạo. Các chương trình resolver có thể sẽ bị can thiệp làm chuyển hướng, gửi thông tin và nhận thông tin tìm kiếm đến một máy chủ DNS Caching giả mạo, điều này sẽ dẫn đến thông tin yêu cầu không có được kết quả chính xác.



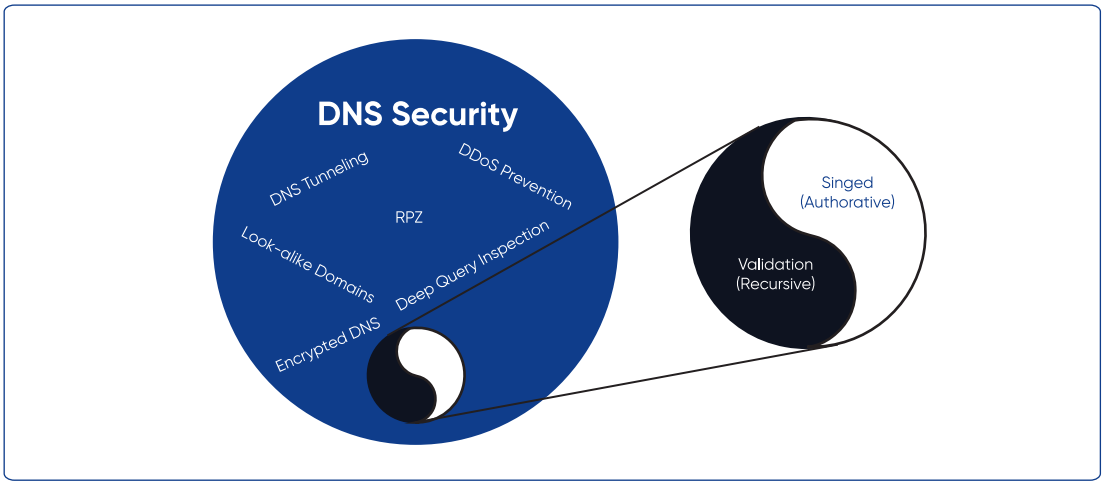
Hình 61: Các vấn đề bảo mật trong hoạt động của hệ thống DNS

Tiêu chuẩn an toàn bảo mật mở rộng cho hệ thống DNS (DNSSEC – DNS Security Extensions) ra đời để giải quyết các vấn đề này. DNSSEC bổ sung chữ ký số vào dữ liệu DNS, đảm bảo rằng mỗi phản hồi DNS có thể được xác minh về tính toàn vẹn và xác thực:

- Xác thực (Authenticity): Đảm bảo phản hồi DNS đến từ nguồn hợp pháp, không phải từ kẻ tấn công.
- Toàn vẹn (Integrity): Đảm bảo dữ liệu không bị thay đổi trong quá trình truyền tải.

Khi DNSSEC được triển khai đầy đủ, mọi phản hồi DNS đều có thể được xác minh và tin cậy, loại bỏ hoàn toàn nguy cơ tấn công giả mạo, thay đổi, chuyển hướng người dùng và đặc biệt là dạng tấn công nhiễm độc bộ nhớ đệm (Cache poisoning).

Lưu ý, cần phân biệt, tránh hiểu nhầm giữa DNS Security và DNSSEC. DNS Security là khái niệm rộng, bao gồm nhiều vấn đề, các biện pháp và chiến lược để bảo vệ hệ thống DNS khỏi các mối đe dọa và tấn công mạng. Trong khi đó, DNSSEC chỉ là một phần trong số các biện pháp này, là một tập hợp các tiêu chuẩn mở rộng cho giao thức DNS, nhằm cung cấp tính toàn vẹn và xác thực cho dữ liệu DNS[11] .



Hình 62: Phân biệt DNS Security và DNSSEC

Như vậy có thể thấy DNSSEC bao gồm 02 quá trình:

1) Quá trình xác thực (Validating):

- Chức năng: Khi một máy khách gửi yêu cầu DNS đến một máy chủ DNS, quá trình xác thực sẽ kiểm tra các chữ ký số (digital signatures) để đảm bảo rằng dữ liệu nhận được không bị thay đổi và đến từ một nguồn đáng tin cậy.
- Cách hoạt động: Máy chủ DNS sẽ kiểm tra các bản ghi DNS và chữ ký số tương ứng. Nếu chữ ký hợp lệ, máy chủ sẽ xác thực rằng dữ liệu là chính xác trước khi gửi phản hồi về cho máy khách.

2) Quá trình ký (Signing):

- Chức năng: Quá trình này liên quan đến việc tạo ra chữ ký số cho các bản ghi DNS trên máy chủ DNS chính (master server).
- Cách hoạt động: Khi dữ liệu DNS được cập nhật, máy chủ sẽ sử dụng khóa riêng (private key) để ký các bản ghi DNS. Chữ ký này sau đó sẽ được lưu trữ cùng với các bản ghi và có thể được xác thực bởi các máy chủ DNS khác.

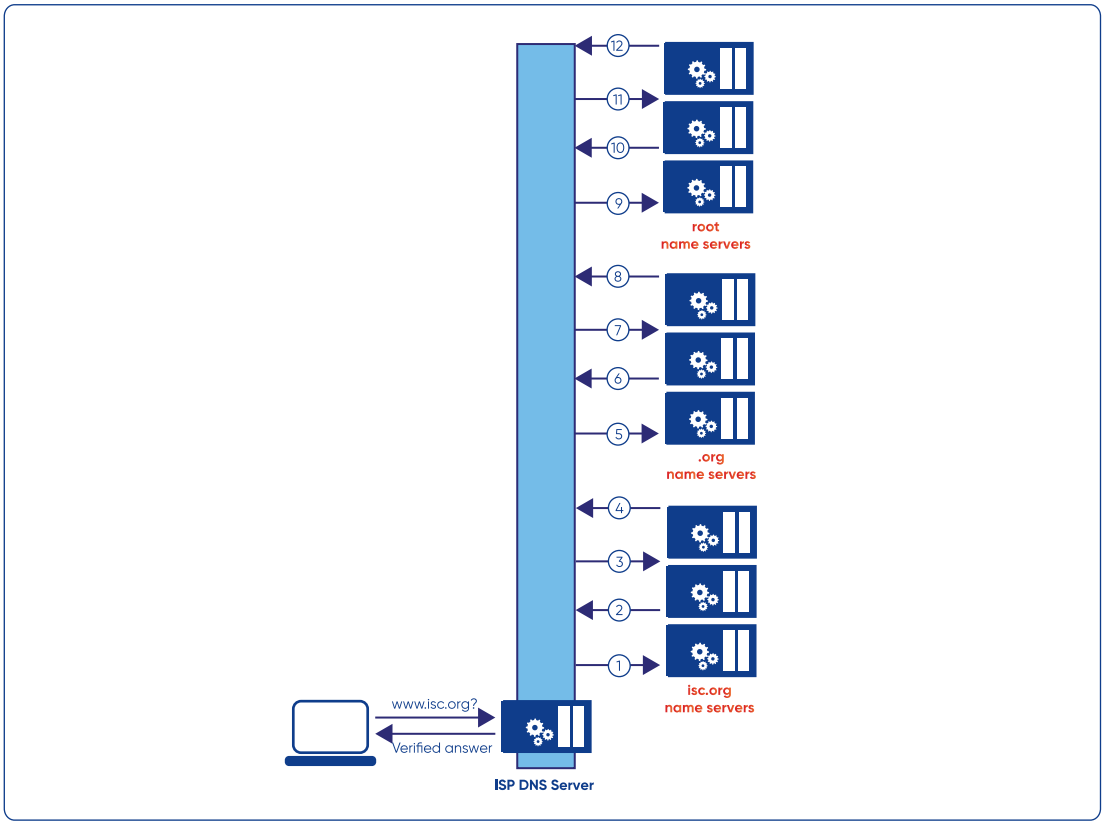
Lưu ý về DNSSEC:

- *Không thực hiện mã hóa dữ liệu: Mặc dù DNSSEC sử dụng các khóa mã hóa trong quá trình ký và xác thực, nó không mã hóa dữ liệu DNS. Điều này có nghĩa là thông tin vẫn có thể được nhìn thấy trong quá trình truyền tải, nhưng tính toàn vẹn và xác thực của dữ liệu được đảm bảo thông qua chữ ký số.*
- *Mục đích chính: Mục tiêu của DNSSEC là bảo vệ người dùng khỏi các cuộc tấn công giả mạo DNS và đảm bảo rằng thông tin mà họ nhận được là chính xác và không bị can thiệp.*

a. Quá trình truy vấn và được xác thực với DNSSEC:

Hình 63 là sơ đồ thể hiện quá trình truy vấn và trả lời truy vấn đối với DNS có DNSSEC:

[11] Thông số kỹ thuật của DNSSEC được mô tả ban đầu trong ba RFC: RFC 4033, 4034, và 4035.



Hình 63: Quá trình truy vấn và được xác thực với DNSSEC

Đối với quá trình truy vấn có DNSSEC, các bước thực hiện truy vấn sẽ theo trình tự như đối với các truy vấn DNS thông thường. Và sau khi máy chủ tên miền đệm (ISP DNS Server) nhận được câu trả lời cuối cùng về thông tin máy chủ tền miền cần truy vấn từ máy chủ Authoritative DNS Server. Máy chủ tên miền đệm (ISP DNS Server) sẽ thực hiện chức năng xác thực DNSSEC.

(1) Máy chủ DNS của ISP gửi yêu cầu truy vấn bản ghi A của tên miền www.isc.org đến các máy chủ tên miền isc.org.

(2) Máy chủ DNS của ISP đó sẽ phản hồi lại bằng câu trả lời kèm theo bản ghi tài nguyên RRSIG (chữ ký số) của bản ghi A.

(3) Máy chủ DNS của ISP tiếp tục truy vấn bản ghi tài nguyên DNSKEY của tên miền isc.org lên chính các máy chủ tên miền isc.org

(4) Máy chủ tên miền isc.org sẽ phản hồi lại câu trả lời kèm theo các bản ghi DNSKEY và RRSIG của bản ghi DNSKEY.

(5) Máy DNS của ISP truy vấn bản ghi DS của isc.org đến máy chủ tên miền .org

(6) Máy chủ tên miền .org phản hồi lại bản ghi DS và RRSIG của tên miền isc.org.

(7) Máy chủ DNS của ISP truy vấn bản ghi DNSKEY của tên miền .org đến chính các máy chủ tên miền .org

(8) Máy chủ tên miền .org sẽ phản hồi lại bản ghi DNSKEY và RRSIG của DNSKEY.

(9) Máy chủ DNS của ISP truy vấn bản ghi DS của tên miền .org lên các máy chủ ROOT.

(10) Máy chủ ROOT sẽ phản hồi lại bản ghi DS kèm theo chữ ký RRSIG của DS.

(11) Máy chủ DNS của ISP tiếp tục hỏi bản ghi DNSKEY của tên miền cấp cao nhất "." lên chính các máy chủ ROOT.

(12) Máy chủ ROOT sẽ phản hồi lại bản ghi DNSKEY của tên miền "." kèm theo bản ghi RRSIG của DNSKEY.

Sau khi xác minh được câu trả lời cuối dùng đã được xác thực, máy chủ DNS của ISP sẽ gửi lại thông tin câu trả lời cho máy khách (client).

b. Phản hồi của DNSSEC đối với máy khách (client):

Ở bước cuối cùng trong Hình trên, bộ phân giải xác thực phản hồi cho máy khách theo ba cách[12] có thể xảy ra:

- Bảo mật (Secure): Tên miền đích đã triển khai DNSSEC và bộ phân giải xác thực đã kiểm tra và xác thực đảm bảo câu trả lời có thể được tin tưởng hoàn toàn.

[12] RFC 4034, Mục 5: Theo tiêu chuẩn RFC 4034, có bốn loại phản hồi có thể xảy ra, loại thứ tư là không xác định (indeterminate). Tuy nhiên, hầu hết các máy chủ DNSSEC chỉ gửi ba loại phản hồi đã đề cập ở trên.

- Không bảo mật (Insecure): Tên miền đích chưa triển khai DNSSEC, và bộ phân giải xác thực sẽ không thực hiện bước xác thực DNSSEC mà quay trở lại phương thức phân giải DNS truyền thống/không bảo mật. Do đó, câu trả lời không được xác thực và không đảm bảo an toàn.
- Giả mạo (Bogus): Tên miền đích đã triển khai DNSSEC, nhưng trong quá trình xác thực, bộ phân giải xác thực phát hiện ra lỗi. Tên miền này có thể bị cấu hình sai hoặc đã bị tấn công thay đổi thông tin. Tại máy khách (client) có thể nhận được mã phản hồi với mã lỗi SERVFAIL.

1.2. Các bản ghi mới trong DNSSEC

DNSSEC là công nghệ an toàn mở rộng của DNS, về bản chất DNSSEC cung cấp các cơ chế có khả năng chứng thực và đảm bảo toàn vẹn dữ liệu cho hệ thống DNS, theo đó DNSSEC đưa ra 4 loại bản ghi mới:

- Bản ghi khóa công cộng DNS (DNSKEY - DNS Public Key): sử dụng để chứng thực zone dữ liệu.
- Bản ghi chữ ký tài nguyên (RRSIG - Resource Record Signature): sử dụng để chứng thực cho các bản ghi tài nguyên trong zone dữ liệu.
- Bản ghi bảo mật kế tiếp (NSEC - Next Secure): sử dụng trong quá trình xác thực đối với các bản ghi có cùng sở hữu tập các bản ghi tài nguyên hoặc bản ghi CNAME. Kết hợp với bản ghi RRSIG để xác thực cho zone dữ liệu.
- Bản ghi ký ủy quyền (DS - Delegation Signer): thiết lập chứng thực giữa các zone dữ liệu, sử dụng trong việc ký xác thực trong quá trình chuyển giao DNS.

Mục tiêu đặt ra là DNSSEC không làm thay đổi tiến trình truyền dữ liệu DNS và quá trình chuyển giao từ các DNS cấp cao xuống các DNS cấp thấp hơn, mặt khác đối với các máy trạm (resolver) cần yêu cầu đáp ứng hỗ trợ các cơ chế mở rộng này. Một zone dữ liệu được ký xác thực sẽ chứa đựng một trong các bản ghi RRSIG, DNSKEY, NSEC và DS.

Như vậy bằng cách thức tổ chức thêm những bản ghi mới và những giao thức đã được chỉnh sửa nhằm chứng thực nguồn gốc và tính toàn vẹn dữ liệu cho hệ thống, với DNSSEC, hệ thống DNS đã được mở rộng thêm các tính năng bảo mật và được tăng cường độ an toàn, tin cậy, khắc phục được những nhược điểm của thiết kế sơ khai ban đầu. Vừa đáp ứng được các yêu cầu thông tin định tuyến về tên miền, giao thức làm việc giữa các máy chủ DNS với nhau, vừa đáp ứng được các yêu cầu bảo mật, tăng cường khả năng dự phòng cho hệ thống.

Các bản ghi trong DNSSEC được khai báo trong các zone dữ liệu để chứng thực thông tin trong zone dữ liệu đó, đảm bảo độ tin cậy trong quá trình trao đổi thông tin cũng như truy vấn tìm kiếm DNS. Trong khi vẫn đảm bảo hoạt động bình thường của các bản ghi tài nguyên DNS thông thường thì các bản ghi DNSSEC cần khai báo chính xác và thông tin xác thực phải đồng bộ.

DNSSEC đưa ra khái niệm ký zone (Zone Signing): một zone được ký bao gồm khóa công cộng DNS (DNS Public Key), chữ ký bản ghi tài nguyên (RRSIG), bảo mật tiếp theo (NSEC), và ký chuyển giao (Delegation Signer). Một zone mà không thêm những bản ghi này vào là một zone chưa được ký. Đồng thời DNSSEC đòi hỏi thay đổi định nghĩa của bản ghi tài nguyên CNAME bằng 2 bản ghi chứng thực là bản ghi RRSIG và bản ghi NSEC.

a. Thêm bản ghi DNSKEY vào một zone

Để ký một zone, người quản trị zone sẽ tạo một hay nhiều cặp khóa công cộng/dành riêng (public/private), cặp khóa công cộng dùng cho zone chính và khóa riêng để ký cho những bản ghi cần xác thực trong zone. Mỗi zone phải thêm một bản ghi DNSKEY (zone DNSKEY RR) chứa đựng khóa công cộng tương ứng, và mỗi khóa riêng được dùng để tạo bản ghi RRSIG trong zone.

Bản ghi chứng thực DNSKEY cho zone phải có bit Zone Key của trường dữ liệu cờ đặt giá trị là 1. Nếu quản trị zone có ý định ký một zone để chứng thực thì zone chính phải chứa đựng ít nhất một bản ghi DNSKEY để hoạt động như một điểm bảo mật ở trong zone. Điểm bảo mật được dùng cùng với bản ghi DS tương ứng ở zone cha trong hoạt động chuyển giao DNS.

b. Thêm các bản ghi RRSIG vào một zone

Với một zone đã được ký bởi bản ghi DNSKEY, thì các bản ghi tài nguyên trong zone đó cần có một bản ghi RRSIG ký xác thực. Một bản ghi tài nguyên có thể có nhiều bản ghi RRSIG kết hợp với nó. Các bản ghi RRSIG chứa chữ ký điện tử kết hợp chặt chẽ với các bản ghi tài nguyên để xác thực cho các bản ghi tài nguyên đó. Đặc biệt, giá trị TTL trong các bản ghi RRSIG với một tên miền sở hữu không giống với giá trị TTL của bản ghi tài nguyên.

Trong trường hợp các bản ghi tài nguyên cùng sở hữu một tên miền thì cần kết hợp bản ghi RRSIG với bản ghi NSEC để xác thực, trường hợp này cũng tương tự đối với bản ghi CNAME.

Tập bản ghi tài nguyên NS trong zone phải được ký xác thực, khi bản ghi NS là bản ghi chuyển giao từ máy chủ tên miền cha xuống máy chủ tên miền con thì cần kết hợp bản ghi RRSIG với bản ghi xác thực DS. Bản ghi glue cũng cần xác thực bằng RRSIG.

c. Thêm bản ghi NSEC vào một zone

Mỗi tên miền sở hữu nhiều hơn 1 bản ghi tài nguyên cùng loại trong một zone hoặc một tập bản ghi NS chuyển giao thì phải có một bản ghi NSEC để xác thực. Trong đó, giá trị TTL nhỏ nhất cho một bản ghi NSEC phải bằng với giá trị TTL trong bản ghi SOA của zone đó.

Một bản ghi NSEC và bản ghi RRSIG kết hợp với nó không nhất thiết là bản ghi duy nhất cho bất cứ tên miền sở hữu bản ghi bảo mật nào. Vì thế, qui trình ký không phải tạo bất cứ bản ghi RRSIG hoặc NSEC nào cho những tên miền sở hữu bản ghi mà không sở hữu bất cứ tập bản ghi nào trước khi zone được ký. Lý do chính là muốn ổn định giữa không gian đã ký và không gian chưa ký của một zone và mong giảm rủi ro đối với những mâu thuẫn trong phản hồi những máy chủ truy vấn đệ qui không được cấu hình bảo mật.

Các bản ghi RRSIG hiện diện tại tên miền sở hữu các tập bản ghi mà nó nắm giữ. Các bản ghi NSEC hiện diện tại tên miền sở hữu và còn hiện diện tại điểm chuyển giao của các tên miền con của chúng. Vì thế, bất cứ tên miền nào có một tập bản ghi NSEC sẽ có các bản ghi RRSIG trong zone được ký.

d. Thêm bản ghi DS vào trong một zone

Bản ghi DS thiết lập chứng thực giữa những zone DNS. Một bản ghi DS được biểu diễn cho bản ghi chuyển giao khi zone con được ký. Bản ghi DS kết hợp với bản ghi RRSIG để chứng thực cho zone được chuyển giao tại máy chủ tên miền cha. Bản ghi DS được khai báo trước, và bản ghi RRSIG khai báo sau giống như khai báo để xác thực cho một bản ghi tài nguyên thông thường.

Trường TTL của tập bản ghi DS phải ứng với trường TTL của tập bản ghi NS ủy quyền (có nghĩa là tập bản ghi NS trong cùng zone chứa tập bản ghi DS). Việc xây dựng một bản ghi DS đòi hỏi phải có hiểu biết của bản ghi DNSKEY tương ứng trong zone con để đưa ra được các giao tiếp giữa zone con và zone cha.

e. Những thay đổi đối với bản ghi CNAME

Nếu một tập bản ghi CNAME hiện diện tại một tên miền trong một zone được ký, sẽ thay thế bằng tập bản ghi RRSIG và NSEC tương ứng trong tên miền đó. Đây là một phiên bản đã được chỉnh sửa của định nghĩa CNAME nguyên gốc. Định nghĩa nguyên gốc của bản ghi CNAME không cho phép bất cứ kiểu nào khác cùng tồn tại với bản ghi CNAME, nhưng một zone được ký đòi hỏi những bản ghi NSEC và bản ghi RRSIG cho mọi tên miền. Để giải quyết xung đột này, định nghĩa của bản ghi CNAME của hệ thống DNS đã được chỉnh sửa lại để cho phép nó cùng tồn tại với các bản ghi NSEC và bản ghi RRSIG.

DNSKEY được thiết lập để tạo khóa công cộng nhằm thực hiện xác thực với các máy chủ DNS khác có cùng khóa công cộng này. Các bản ghi chứng thực RRSIG sử dụng để ký xác thực cho các bản ghi tài nguyên SOA, A, MX... Đối với các bản ghi NS khai báo quyền sở hữu tên miền đối với tên miền gốc thì sử dụng bản ghi NSEC kết hợp với bản ghi RRSIG để xác thực. Đối với các bản ghi chuyển giao từ DNS cha xuống các máy chủ tên miền DNS con thì kết hợp với bản ghi DS với bản ghi RRSIG để xác thực.

2. Tính năng và ứng dụng của DNSSEC

DNSSEC bổ sung bốn tính năng mới mà hệ thống DNS truyền thống không có:

- Xác thực – Authenticity: Còn được gọi là xác thực nguồn gốc dữ liệu DNS, bằng cách sử dụng chữ ký số và khóa mật mã, các máy chủ Authoritative DNS Server lưu trữ các tên miền được ký bằng DNSSEC có thể phản hồi với dữ liệu đã được ký số, giúp chứng minh tính xác thực của dữ liệu với những bên khác.
- Toàn vẹn dữ liệu – Data Integrity: Đảm bảo nội dung, dữ liệu DNS không thay đổi trong quá trình truyền. Các máy chủ Authoritative DNS Server hỗ trợ DNSSEC phản hồi truy vấn với cả câu trả lời dạng văn bản thuần (plaintext) và chữ ký số. Các trình phân giải đệ quy hỗ trợ DNSSEC (còn gọi là bộ phân giải xác thực) có thể tính toán chữ ký số, từ đó xác minh rằng dữ liệu thuần chưa bị thay đổi trong quá trình truyền.
- Chuỗi tin cậy – Chain of Trust: DNSSEC tận dụng cấu trúc phân cấp của DNS, cho phép các bộ phân giải xác thực kiểm tra mối quan hệ tin cậy giữa các tên miền con (ví dụ: vnnic.vn) và miền cha (.vn) cho đến khi đạt đến một điểm neo tin cậy được cấu hình rõ ràng (thường là DNS Root). Phương pháp này yêu cầu tải lên thông tin bản ghi ký chuyển giao (DS – Delegation Signer) của zone tên miền con "child zone" vào zone cha "parent zone" để kết nối hoàn thành chuỗi tin cậy. Quá trình này được thực hiện thông qua bản ghi Delegation Signer (DS) trong zone cha, chứa giá trị băm của Khóa ký công khai (KSK), được lưu dưới dạng bản ghi DNSKEY trong zone con "child zone".
- Chứng minh sự không tồn tại – Proof of Non-Existence: Với DNSSEC, khi một trình phân giải đệ quy xác thực các truy vấn DNSSEC đối với một tên miền không tồn tại, máy chủ có thể chứng minh điều đó một cách rõ ràng, thay vì chỉ phản hồi NXDOMAIN. Tính năng này giúp ngăn chặn các kịch bản mà kẻ tấn công gây ra từ chối dịch vụ (DoS) bằng cách giả mạo các phản hồi DNS, chẳng hạn như gửi một phản hồi lỗi cho người dùng rằng www.google.com. không tồn tại, trong khi tên miền vẫn hoạt động một cách bình thường.

3. Làm rõ những hiểu lầm về DNSSEC

Nhiều người có những cách hiểu nhầm lẫn hoặc chưa chính xác về DNSSEC, một phần là do tên gọi của nó dễ gây nhầm lẫn. Trên thực tế, DNSSEC là một giải pháp bảo mật được thiết kế đặc biệt để tăng cường tính toàn vẹn và xác thực dữ liệu trong hệ thống DNS. Cơ chế này giúp ngăn chặn các hình thức tấn công như giả mạo bản ghi DNS, thay đổi nội dung truy vấn, hoặc chuyển hướng người dùng đến các địa chỉ độc hại. Một trong những mối nguy hiểm mà DNSSEC giúp bảo vệ là **cache poisoning**, hay còn gọi là đầu độc bộ nhớ đệm. Tấn công này xảy ra khi kẻ tấn công chèn dữ liệu sai vào bộ nhớ đệm của DNS resolver, khiến người dùng bị chuyển hướng đến các trang web độc hại. Dưới đây là một số nhầm lẫn phổ biến về DNSSEC.

a. DNSSEC cung cấp quyền riêng tư, mã hóa dữ liệu

Quan niệm sai lầm phổ biến nhất về DNSSEC là nó cung cấp quyền riêng tư, mã hóa dữ liệu. Không khó để hiểu tại sao nhiều người nghĩ vậy, bởi vì chúng ta thường thấy các thuật ngữ như "khóa mật mã" (cryptographic keys) và "bảo mật" (security). Tuy nhiên, DNSSEC chỉ sử dụng mật mã khóa công khai để xác thực, không phải để bảo mật mã hóa dữ liệu DNS. Điều này có nghĩa là bất kỳ ai cũng có thể thấy câu trả lời ở dạng văn bản thuần (plaintext), cùng với chữ ký số (RRSIG) được sử dụng để xác thực.

b. DNSSEC cần chứng thư số hoặc hạ tầng PKI

Cụm từ "mật mã khóa công khai" (public key cryptography) có thể khiến nhiều người liên tưởng đến thuật ngữ PKI (hạ tầng khóa công khai - Public Key Infrastructure). Tuy nhiên, thực tế là PKI chủ yếu được thiết kế để phân phối và quản lý khóa thông qua chứng thư số, trong khi DNS – cụ thể là DNSSEC - đã có sẵn cơ chế riêng để phân phối khóa công khai, không phụ thuộc hạ tầng PKI truyền thống.

Vì DNS có sẵn cơ chế xuất bản (public) và phân phối thông tin, nó không phụ thuộc vào bất kỳ hạ tầng PKI bên ngoài nào, chẳng hạn như hệ thống chứng thư số (CA - Certificate Authority). Trong triển khai DNSSEC điển hình, các khóa được tạo, lưu giữ và public công khai ngay trên chính hệ thống máy chủ DNS, mà không cần phải mua chứng thư số từ bên ngoài.

c. DNSSEC bảo vệ người dùng khỏi các tên miền độc hại

DNSSEC là một giao thức, tiêu chuẩn an toàn giúp các máy chủ DNS xác thực phản hồi từ một máy chủ DNS khác. Tuy nhiên, DNSSEC không ngăn chặn kẻ tấn công đăng ký một tên miền độc hại, ký số DNSSEC cho tên miền và sử dụng tên miền đó cho mục đích xấu. Ví dụ:

- Người dùng A đăng ký tên miền attckr.com. và ký số DNSSEC, triển khai DNSSEC trên máy chủ DNS chuyển giao.
- Người dùng B bật tính năng xác thực DNSSEC trên bộ phân giải đệ quy của mình, bộ phân giải này trở thành bộ phân giải xác thực và thực hiện kiểm tra DNSSEC khi phân giải tên miền.
- Người dùng A thiết lập một bản ghi tài nguyên (resource record) cho ftp.attckr.com, trỏ đến địa chỉ IP của máy chủ chứa mã độc.
- Khi người dùng B gửi một truy vấn tìm kiếm địa chỉ IP của ftp.attckr.com. đến trình phân giải đệ quy của mình, máy chủ sẽ sử dụng DNSSEC để xác thực tên miền này. Nếu chữ ký hợp lệ, trình phân giải sẽ xác nhận tên miền này có nguồn gốc xác định.
- Tuy nhiên, DNSSEC không thể và cũng không có chức năng xác định liệu ftp.attckr.com. có phải là một đích đến an toàn hay không.

Nếu muốn lọc bỏ các miền độc hại khỏi hệ thống DNS, thì chúng ta cần phải sử dụng kết hợp các giải pháp công nghệ như RPZ (Response Policy Zones) với DNSSEC để tăng cường, đảm bảo an toàn an ninh.

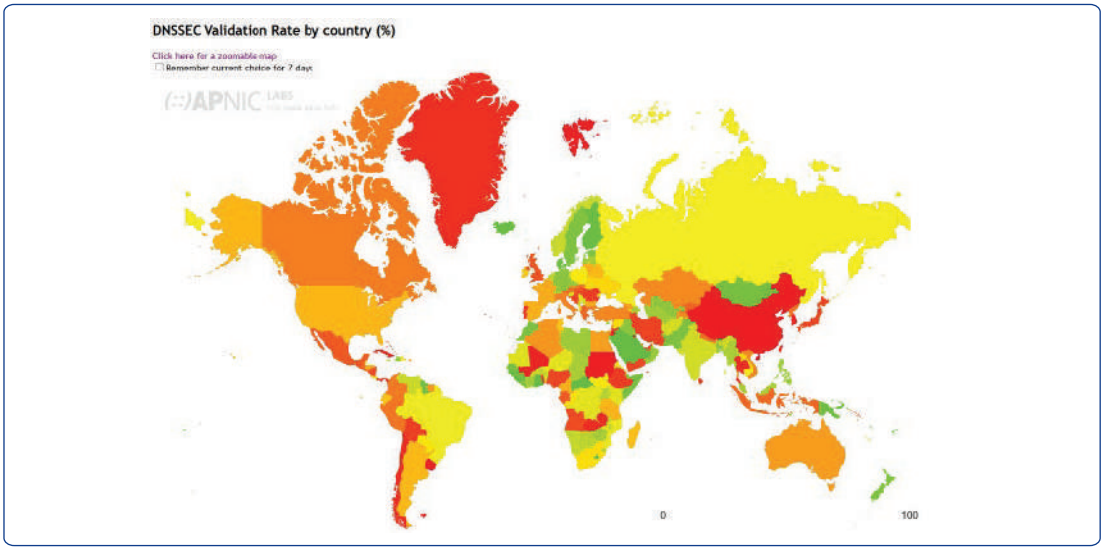
4. Triển khai DNSSEC

4.1. Hiện trạng triển khai

Như đã đề cập ở trên , DNSSEC là một giải pháp an toàn bảo mật được thiết kế đặc biệt để tăng cường tính toàn vẹn và xác thực dữ liệu trong hệ thống DNS. Cơ chế này giúp ngăn chặn các hình thức tấn công như giả mạo bản ghi DNS, thay đổi nội dung truy vấn, hoặc chuyển hướng người dùng đến các địa chỉ độc hại. Tuy nhiên, để DNSSEC thực sự hiệu quả, thì DNSSEC cần được áp dụng triển khai rộng rãi và đồng bộ, nhất quán hơn trên cả các hệ thống Authoritative DNS Server và DNS Recursive.

Theo thống kê của APNIC, tính đến tháng 04/2025 có khoảng 35%[13] các trình phân giải đệ quy (Resolver) hiện nay trên Internet đã bật xác thực DNSSEC (như DNS Google, Cloudflare, Quad9, ...). Một số số liệu xác thực tại các quốc gia như Đức, tỷ lệ xác thực là 80%; Hoa Kỳ là 37%; Úc là 32%; và Việt Nam là 27%.

[13] https://stats.labs.apnic.net/dnssec/XA



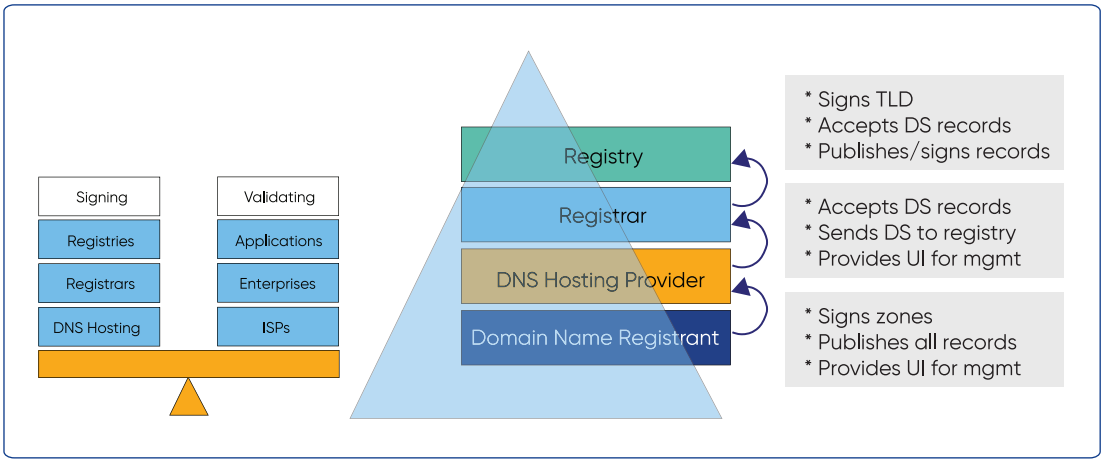
Hình 64: Tỉ lệ xác thực DNSSEC theo quốc gia (APNIC)

Ở phía ký số (signing), tỷ lệ triển khai DNSSEC tại các tên miền cấp miền cao nhất (TLD) theo thống kê của DNSSEC-Tools như sau: .com (4%), .net (~5%), .gov (~15%), ... và tại một số quốc gia có tỉ lệ triển khai DNSSEC cho tên miền ccTLD như sau: .vn (Việt Nam – 1.56%), .nl (Hà Lan - 61%), .ch (Thụy Sĩ – 51%), .cz (Séc – 58%),...

4.2. Triển khai DNSSEC

Đến thời điểm này, chúng ta đã có một cái nhìn rõ ràng về mối đe dọa (giả mạo, chuyển hướng truy cập, nhiễm độc bộ nhớ đệm) và giải pháp khắc phục là áp dụng tiêu chuẩn DNSSEC. Do đó việc lên kế hoạch, phương án triển khai DNSSEC là rất quan trọng và cấp thiết.

Như đã đề cập trước đó, DNSSEC có hai nhóm đối tượng tham gia vào quá trình triển khai DNSSEC là nhóm ký số dữ liệu tên miền (Signing) và nhóm kiểm tra tính xác thực (Validation) của dữ liệu tên miền. Trong đó:



Hình 65: Các thành phần trong triển khai DNSSEC

(1) Nhóm ký số dữ liệu tên miền bao gồm:

- Cơ quan đăng ký tên miền Registry
- Các nhà đăng ký tên miền Registrar
- Các doanh nghiệp cung cấp dịch vụ DNS Hosting
- Các chủ sở hữu đăng ký tên miền

(2) Nhóm kiểm tra dữ liệu tên miền:

- Các ISP, DNS Public
- Các hệ thống máy chủ tên miền đệm của các doanh nghiệp
- Các ứng dụng xác thực với DNSSEC

Chi tiết hướng dẫn triển khai DNSSEC cho từng nhóm đối tượng cụ thể tại: https://vnnic.vn/dns/thong-tin-va-tai-lieu-tham-khao

XIV

DNS ABUSE

1. DNS Abuse là gì

Lạm dụng tên miền (DNS Abuse) là bất kỳ hoạt động nào sử dụng các kỹ thuật, phương thức tấn công liên quan đến tên miền hoặc hệ thống máy chủ tên miền (DNS) trên môi trường mạng để thực hiện các hành vi, hoạt động lừa đảo, có hại hoặc bất hợp pháp. Đây được đánh giá là vấn đề an ninh mạng phức tạp toàn cầu, trở thành vấn đề "nóng" trong việc phát triển, đảm bảo an toàn, tin cậy của Internet.

Lạm dụng tên miền đề cập đến 05 loại hoạt động trực tuyến sử dụng tên miền (domain name) hoặc hệ thống/giao thức DNS (Domain Name System) thực hiện hoạt động có hại hoặc bất hợp pháp, bao gồm: Malware, Botnets, Pharming, Phishing, Spam (trong đó spam được sử dụng như một phương tiện để thực hiện 04 loại trên).

- **Phần mềm độc hại (Malware)** là các phần mềm được cài đặt trên thiết bị mà không có sự đồng ý của người dùng, làm gián đoạn hoạt động của thiết bị, thu thập thông tin nhạy cảm và/hoặc giành quyền truy cập vào hệ thống, máy tính cá nhân. Phần mềm độc hại bao gồm virus, phần mềm gián điệp (spyware), mã độc tống tiền (ransomware) và phần mềm không xác định khác.
- **Botnet** là tập hợp các máy tính kết nối Internet đã bị nhiễm phần mềm độc hại và được lệnh thực hiện các hoạt động dưới sự kiểm soát của tin tặc bằng hình thức kiểm soát từ xa.
- **Lừa đảo (Phishing)** xảy ra khi kẻ tấn công thực hiện các hành vi lừa đảo nạn nhân tiết lộ thông tin cá nhân, công ty hoặc thông tin tài chính nhạy cảm (ví dụ: số tài khoản, ID đăng nhập, mật khẩu), thông qua việc gửi email lừa đảo hoặc email "trông giống" để đánh lừa người dùng cuối truy cập đến các trang web giả mạo (có giao diện giống với giao diện trang web chính thức). Một số chiến dịch lừa đảo nhằm mục đích thuyết phục người dùng cài đặt phần mềm, thực chất là phần mềm độc hại.
- **Giả mạo (Pharming)** là chuyển hướng người dùng đến các trang web hoặc dịch vụ lừa đảo, điển hình là thông qua tấn công hoặc nhiễm độc hệ thống DNS, chiếm quyền điều khiển hệ thống DNS. Việc chiếm quyền điều khiển DNS xảy ra khi những kẻ tấn công sử dụng phần mềm độc hại để chuyển hướng nạn nhân đến trang web của kẻ tấn công thay vì trang web được yêu cầu ban đầu. Nhiễm độc DNS khiến máy chủ DNS hoặc trình phân giải phản hồi bằng một địa chỉ IP giả mạo mang mã độc.
- **Thư rác (Spam)** là các email chứa các loại quảng cáo được gửi tới một danh sách cá nhân và nhóm người dùng, các dạng thư này thường không có ý nghĩa, không có chất lượng thông tin, không được sự đồng ý trước và gây phiền phức cho người dùng. Mặc dù riêng spam không phải là lạm dụng DNS, nhưng nó là "công cụ" được sử dụng để phân phối, phát tán cho các dạng lạm dụng DNS khác.

2. Tác động ảnh hưởng của DNS Abuse

Lạm dụng tên miền (DNS Abuse) đang trở thành một vấn đề ngày càng nghiêm trọng trong môi trường Internet hiện đại. Tình trạng này không chỉ ảnh hưởng đến người dùng cá nhân mà còn gây ra những hệ lụy lớn đối với các tổ chức và doanh nghiệp. Với sự gia tăng của các cuộc tấn công mạng và các hình thức lừa đảo, tác động của DNS Abuse đã trở nên đa dạng và phức tạp. Trong bối cảnh đó, việc hiểu rõ các tác động và ảnh hưởng của DNS Abuse là vô cùng cần thiết để bảo vệ an toàn thông tin cá nhân, duy trì độ tin cậy của dịch vụ trực tuyến, và đảm bảo sự ổn định của hạ tầng Internet toàn cầu.

- Tác động đến người dùng: Lạm dụng tên miền (DNS Abuse) gây ra nguy cơ mất thông tin cá nhân, giảm độ tin cậy của Internet, ảnh hưởng trực tiếp đến trải nghiệm và an toàn thông tin đối với người dùng.
- Tác động đến tổ chức, doanh nghiệp: Việc lạm dụng tên miền dẫn đến mất uy tín, gây thiệt hại kinh tế và tăng nguy cơ tấn công mạng đối với tổ chức, doanh nghiệp. Nó cũng ảnh hưởng đến cơ sở hạ tầng Internet và có thể gây ra rủi ro pháp lý, cản trở phát triển công nghệ mới.
- Tác động đến an toàn thông tin mạng và xã hội: Lạm dụng tên miền có thể gây ra các cuộc tấn công quy mô lớn, làm gián đoạn dịch vụ công cộng và ảnh hưởng đến an toàn xã hội. Nó cũng dẫn đến thiệt hại kinh tế lớn cho doanh nghiệp, đặc biệt trong lĩnh vực thương mại điện tử, và đe dọa sự ổn định của Internet toàn cầu.

3. Giải pháp ngăn chặn, giảm thiểu DNS Abuse

Vấn đề lạm dụng tên miền trực tuyến (DNS Abuse) là một vấn đề phức tạp, quan trọng. Trên cơ sở nghiên cứu, phân tích kinh nghiệm và thực tiễn triển khai tại các tổ chức, quốc gia trên thế giới, đặc biệt là của ICANN cho thấy, để giảm thiểu, ngăn chặn việc lạm dụng tên miền (DNS Abuse) cần phải triển khai đồng bộ, kết hợp nhiều giải pháp khác nhau, trong đó tập trung:

a. Nhóm các giải pháp quy định, chính sách:

- Chính sách và quy định: xây dựng và thực thi một cách có hiệu quả các chính sách về quản lý tên miền và ngăn chặn lạm dụng. Tập trung triển khai các quy định giúp quản lý các nhà đăng ký tên miền và đảm bảo họ thực hiện các biện pháp phù hợp trong xử lý tên miền lạm dụng.
- Cơ chế giám sát, kiểm tra: có cơ chế để theo dõi và đánh giá hoạt động của các nhà đăng ký tên miền, nhằm đảm bảo rằng các quy định được tuân thủ và phát hiện kịp thời các hành vi lạm dụng.
- Hợp tác quốc tế: tăng cường hợp tác giữa các quốc gia và tổ chức quốc tế, chia sẻ thông tin về các trường hợp lạm dụng và các biện pháp phản ứng hiệu quả.
- Giáo dục và nâng cao nhận thức: tổ chức các chương trình đào tạo và hội thảo cho các bên liên quan (nhà đăng ký, người sử dụng, cơ quan thực thi pháp luật) về các vấn đề liên quan đến lạm dụng tên miền và cách phòng ngừa.

b. Nhóm các giải pháp về kỹ thuật:

Các giải pháp được sử dụng nhằm đảm bảo an toàn bảo mật cho chính hệ thống DNS, giao thức DNS đều hướng tới mục tiêu chung: Ngăn chặn, giảm thiểu các nguy cơ, các cuộc tấn công bằng các phương thức kỹ thuật nhắm tới các hệ thống DNS (DNS Cache poisoning, DDoS, DNS Hijacking, DNS Tunneling, ...).

- Triển khai hệ thống tiếp nhận, phân tích, xử lý các báo cáo lạm dụng tên miền từ người dùng Internet (hệ thống DNS Abuse Report Portal).
- Triển khai các công nghệ, tiêu chuẩn kỹ thuật nhằm kiểm soát, ngăn chặn việc đăng ký tên miền cho mục đích xấu: trong đó tập trung vào việc thực hiện xác thực chủ thể đăng ký tên miền thông qua áp dụng các công nghệ như định danh khách hàng điện tử (eKYC, eID), kết nối với CSDL quốc gia về dân cư, giúp xác thực chặt chẽ cho các yêu cầu đăng ký tên miền, bao gồm xác minh danh tính và địa chỉ của chủ thể đăng ký.
- Triển khai các giải pháp công nghệ, tiêu chuẩn kỹ thuật nhằm tăng cường đảm bảo an toàn, hạ tầng DNS (như DNSSEC, DNS Anycast, DNS Firewall, ...). Việc triển khai DNSSEC nhằm đảm bảo tính toàn vẹn và xác thực của dữ liệu DNS, giúp ngăn chặn các cuộc tấn công chuyển hướng đến các website giả mạo (cache poisoning). Triển khai hệ thống tên miền phân tán (DNS Anycast) giúp giảm thiểu rủi ro từ các cuộc tấn công DDoS và tăng cường khả năng chịu lỗi.
- Ứng dụng công nghệ trong giám sát, phân tích lưu lượng nhằm phát hiện các hành vi, nguy cơ lạm dụng tên miền.

Bên cạnh đó, cần tăng cường triển khai các giải pháp công nghệ, kỹ thuật khác như: hệ thống lọc và bảo mật DNS (DNS Firewall, DNS RPZ) sử dụng các công nghệ lọc DNS để chặn truy cập đến các tên miền độc hại hoặc lừa đảo, bảo vệ người dùng khỏi các mối đe dọa. Triển khai các hệ thống phát hiện xâm nhập (IDS) để theo dõi và phát hiện các hoạt động bất thường trong hệ thống DNS, giúp phát hiện sớm các cuộc tấn công. Công nghệ mã hóa sử dụng các giao thức bảo mật như TLS để mã hóa dữ liệu truyền tải, bảo vệ thông tin cá nhân và ngăn chặn các cuộc tấn công man-in-the-middle, ...

Nội dung phân tích chi tiết các giải pháp này như đã trình bày tại các Mục XI, XII.4 và XIII của cuốn sách này.

c. Nhóm các giải pháp khác:

- Chính sách quản lý tên miền: xây dựng các chính sách quản lý tên miền chặt chẽ, bao gồm quy trình xác minh danh tính và thông tin người đăng ký để ngăn chặn việc đăng ký tên miền cho mục đích lạm dụng.
- Đánh giá rủi ro và phân tích dữ liệu: thực hiện các phân tích định kỳ về rủi ro liên quan đến tên miền để xác định các lỗ hổng và cải thiện các biện pháp bảo vệ.
- Tăng cường trách nhiệm của các nhà đăng ký: khuyến khích các nhà đăng ký tên miền thực hiện trách nhiệm của họ trong việc giám sát và phát hiện các hành vi lạm dụng, đồng thời cung cấp các kênh báo cáo cho người dùng.

Việc kết hợp các giải pháp về quy định chính sách, kỹ thuật, ... là rất quan trọng để đối phó hiệu quả với vấn đề lạm dụng tên miền. Sự hợp tác giữa các bên liên quan và việc triển khai các quy định chính sách và công nghệ hiện đại sẽ giúp bảo vệ an toàn cho môi trường Internet và giảm thiểu các rủi ro liên quan đến lạm dụng tên miền (DNS Abuse).

XV

CÁC CÔNG NGHỆ MỚI TRONG DNS

1. Các công nghệ mới trong DNS

1.1. DNSSEC và Blockchain-Based DNS

Nội dung chi tiết về DNSSEC như đã trình bày tại Mục III Phần 2 của cuốn sách này.

Bảo mật luôn là mối quan tâm hàng đầu trong các hệ thống DNS. DNS Security Extensions (DNSSEC) là một cơ chế quan trọng giúp đảm bảo tính xác thực và toàn vẹn của các phản hồi DNS bằng cách sử dụng chữ ký mật mã, giảm thiểu đáng kể các mối đe dọa như tấn công cache poisoning và giả mạo DNS. Mặc dù trước đây việc triển khai còn chậm do sự phức tạp về kỹ thuật, công nghệ và quản lý, nhưng gần đây các công cụ tự động hóa đã giúp thúc đẩy sự phổ biến của DNSSEC. Ngoài ra, các giải pháp DNS dựa trên blockchain như Handshake (HNS), Ethereum Name Service (ENS), và Unstoppable Domains cung cấp các lựa chọn thay thế phi tập trung, tăng cường bảo mật bằng cách loại bỏ các điểm lỗi đơn và hạn chế kiểm duyệt nội dung. Nhằm mục tiêu mở rộng hệ thống DNS truyền thống, hệ thống BNS là hệ thống ứng dụng công nghệ blockchain trong quản lý và lưu trữ tên miền.

Hệ thống BNS không sử dụng cơ chế quản lý tên miền tập trung như DNS truyền thống, thay vào đó hệ thống sử dụng blockchain để quản lý tên miền một cách phi tập trung (decentralized management). Toàn bộ thông tin tên miền sẽ được lưu trữ trên các chuỗi khối (blockchain), do đó giúp tăng tính minh bạch và an toàn. Người sử dụng có thể trực tiếp sở hữu và quản lý tên miền của mình, không phụ thuộc vào bên thứ ba. Hệ thống BNS có thể được tích hợp với các ứng dụng blockchain khác, cho phép người sử dụng tên miền có thể truy cập trực tiếp các dịch vụ trên blockchain. Như vậy, hệ thống BNS sẽ bao gồm tính phi tập trung, minh bạch, sở hữu người dùng và khả năng tích hợp với ứng dụng blockchain, qua đó giải quyết một số hạn chế của hệ thống DNS truyền thống. Hiện nay Hệ thống tên miền blockchain vẫn đang trong giai đoạn nghiên cứu, thử nghiệm.

1.2. Mã hóa DNS

Nội dung chi tiết về mã hóa DNS như đã trình bày tại Mục II Phần 2 của cuốn sách này.

Các truy vấn và phản hồi truy vấn DNS truyền thống từ lâu đã dễ bị nghe lén và dễ dàng bị thay đổi thông tin do chúng được gửi đi mà không mã hóa. Để khắc phục vấn đề này, các giao thức mã hóa hiện đại đã xuất hiện. **DNS-over-HTTPS (DoH)** mã hóa các truy vấn DNS bằng HTTPS, giúp ngăn chặn việc nghe lén từ các nhà cung cấp dịch vụ Internet (ISP) hoặc tin tặc. **DNS-over-TLS (DoT)** sử dụng giao thức TLS để mã hóa truy vấn DNS, đảm bảo quyền riêng tư. **DNS-over-QUIC (DoQ)**, một bước tiến mới, sử dụng QUIC – giao thức truyền tải hiện đại giúp giảm độ trễ và cải thiện độ tin cậy, rất hữu ích cho các ứng dụng thời gian thực (IETF RFC 9250).

1.3. Trí tuệ nhân tạo và học máy

Trí tuệ nhân tạo (AI) và học máy (ML) đang được ứng dụng ngày càng nhiều trong việc nâng cao bảo mật DNS. Các mô hình AI tiên tiến có thể phân tích lưu lượng DNS theo thời gian thực, phát hiện các bất thường như malware sử dụng thuật toán tạo tên miền (DGA), botnet C2, và tên miền lừa đảo. Ngoài ra, các dịch vụ lọc DNS tích hợp AI có thể chủ động chặn các tên miền độc hại, giúp cải thiện bảo mật mạng doanh nghiệp.

1.4. Post-Quantum Cryptography

Post-Quantum Cryptography (PQC), hay mật mã hậu lượng tử, là lĩnh vực nghiên cứu các thuật toán mã hóa mới nhằm bảo vệ dữ liệu trước các mối đe dọa từ máy tính lượng tử trong tương lai. Các máy tính lượng tử, dựa trên cơ chế tính toán lượng tử (Quantum Computing), có khả năng phá vỡ nhanh chóng các thuật toán mật mã bất đối xứng phổ biến hiện nay như RSA và ECC (Elliptic Curve Cryptography), nhờ thuật toán lượng tử Shor. Vì vậy, việc xây dựng các thuật toán mã hóa "kháng lượng tử" trở thành một ưu tiên chiến lược về bảo mật trong những năm gần đây.

DNSSEC (Domain Name System Security Extensions) là công nghệ quan trọng nhằm bảo vệ tính toàn vẹn và xác thực dữ liệu DNS thông qua việc sử dụng các thuật toán mã hóa bất đối xứng (RSA hoặc ECC) để ký số các bản ghi DNS. Các thuật toán này hiện nay đều rất an toàn, nhưng sẽ dễ dàng bị phá vỡ khi máy tính lượng tử đủ mạnh xuất hiện. Điều này gây ra mối đe dọa nghiêm trọng, bởi việc phá vỡ DNSSEC đồng nghĩa với việc giả mạo

tên miền, làm mất niềm tin của người dùng, dẫn tới nguy cơ tấn công giả mạo, lừa đảo, đánh cắp thông tin, hay thậm chí đánh sập hệ thống mạng diện rộng.

Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) đang thực hiện dự án Post-Quantum Cryptography nhằm tiêu chuẩn hóa các thuật toán mã hóa kháng lượng tử. Các nhà nghiên cứu đã bắt đầu thử nghiệm việc tích hợp PQC vào DNSSEC. Một số dự án thử nghiệm thực tế (Proof of Concept) đã được tiến hành. Ví dụ, dự án của SIDN Labs (Hà Lan) vào năm 2022 đã thử nghiệm chữ ký DNSSEC bằng thuật toán SPHINCS+ trên hệ thống DNS công cộng và bước đầu cho kết quả khả quan, với chi phí xử lý chấp nhận được. Với tiến độ phát triển của công nghệ lượng tử, việc chuyển đổi sang DNSSEC kháng lượng tử là một yêu cầu cấp bách trong vòng 5-10 năm tới. Các tổ chức quản lý DNS (như ICANN, IETF) đang tích cực thảo luận và chuẩn bị các tiêu chuẩn, giải pháp nhằm thích ứng với sự thay đổi này.

2. DNS và 5G, IoT

2.1. DNS và IoT

2.1.1. DNS trong phân giải tên miền cho IoT

DNS đóng vai trò cốt lõi trên Internet bằng cách chuyển đổi tên miền thành địa chỉ IP, do đó, nó có thể được sử dụng để phân giải định danh IoT. Tương tự như các thiết bị Internet thông thường, các thiết bị IoT được kết nối mạng cũng cần có định danh và một hệ thống để ánh xạ định danh đó thành địa chỉ. Những địa chỉ này sẽ được sử dụng để truy vấn dữ liệu từ thiết bị IoT, điều khiển thiết bị hoặc chuyển hướng đến nguồn thông tin về thiết bị đó.

Các quy ước đặt tên trong IoT rất đa dạng và không tương thích với nhau. Một cách tiếp cận khả thi để giải quyết vấn đề này là chuẩn hóa một quy ước đặt tên toàn cầu cho tất cả thiết bị IoT. Tuy nhiên, điều này gần như không thể thực hiện được vì nhiều ngành công nghiệp như bán lẻ, ô tô và quốc phòng đã sử dụng các hệ thống đặt tên riêng trong nhiều thập kỷ.

Một giải pháp thực tế hơn là giữ nguyên các quy ước đặt tên hiện có và phát triển hệ thống phân giải tên miền chung, trong đó DNS có thể đóng vai trò trung tâm.

- ENUM (Electronic Number Mapping) là một ví dụ điển hình về cách DNS đã từng được sử dụng để ánh xạ số điện thoại thành địa chỉ web.
- Hệ thống phân giải tên đối tượng (Object Name Service - ONS) và Hệ thống phân giải OID (OID Resolution System - ORS) đã cho thấy rằng DNS có thể đăng ký và phân giải định danh duy nhất cho các thiết bị IoT.

Các nghiên cứu về phân giải tên IoT bằng DNS

- Trong công trình nghiên cứu [A Universal Object Name Resolution Scheme for IoT][14] xác định rằng mỗi công nghệ IoT có quy tắc đặt tên riêng và không thể kết nối liền mạch với công nghệ khác, gây ra vấn đề tương thích. Các tác giả đề xuất một cơ chế phân giải tên miền ngang hàng (peer-to-peer equal name resolution), trong đó tên thiết bị từ các công nghệ khác nhau được băm thành chuỗi bit và phân giải qua DNS bằng cách thêm đuôi TLD ".iot".
- Trong công trình nghiên cứu [A DNS Architecture for the Internet of Things][15] đã thử nghiệm cấu trúc tổ chức phân cấp của DNS cho IoT trong lĩnh vực vận tải và logistics, giúp phân giải các URI thành địa chỉ IP để truy xuất thông tin về thiết bị IoT (vị trí, trạng thái, ...).
- Trong công trình nghiên cứu [Exploring the use of DNS as a search engine for the Web of Things][16] đã tận dụng cấu trúc DNS hiện tại để xây dựng công cụ tìm kiếm dành cho Web of Things (WoT). Các tác giả đề xuất sử dụng TLD mới (ví dụ ".env") để cho phép người dùng tìm kiếm dịch vụ IoT trong một phạm vi cụ thể.

Ngoài ra, một số đề xuất giúp cải thiện khả năng định danh tự động cho thiết bị IoT bằng DNS, chẳng hạn như:

- DNS Name Autoconfiguration (DNSNA) giúp tự động cấu hình tên miền DNS trong môi trường IoT sử dụng IPv6.
- DNSNAv4 mở rộng DNSNA cho các thiết bị IoT sử dụng IPv4, cho phép chúng đăng ký tên miền tự động thông qua máy chủ DHCP.

Một số nghiên cứu cũng khai thác phân tích lưu lượng DNS để nhận diện thiết bị IoT:

- IoTFinder là một hệ thống nhận dạng thiết bị IoT bằng cách phân tích lưu lượng DNS thông qua mô hình học máy (machine learning).
- IoTRoam đề xuất một cơ chế chuyển vùng (roaming) cho thiết bị IoT, giúp thiết bị tìm và kết nối với máy chủ Join Server thích hợp bằng DNS.

[14] Yan Z., Kong N., Tian Y., Park Y.J. A Universal Object Name Resolution Scheme for IoT; Proceedings of the 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing; Beijing, China. 20–23 August 2013; pp. 1120–1124. [DOI] [Google Scholar]

[15] Karakostas B. A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics. Procedia Comput. Sci. 2013;19:594–601. doi: 10.1016/j.procs.2013.06.079. [DOI] [Google Scholar]

[16] Kamilaris A., Papakonstantinou K., Pitsillides A. Exploring the use of DNS as a search engine for the Web of Things; Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT); Seoul, Republic of Korea. 6–8 March 2014; Mar 6–8, [DOI] [Google Scholar]

2.1.2. DNS - Giải pháp cho vấn đề đặt tên trong IoT

Hiện tại IoT vẫn chưa có một hệ thống phân giải tên miền toàn cầu thống nhất, và khả năng triển khai một giải pháp duy nhất cho tất cả công nghệ IoT là rất thấp. Tuy nhiên, vấn đề này vẫn có thể được giải quyết một cách thực tế.

Một số giải pháp chấp nhận giữ nguyên các hệ thống đặt tên hiện có và xây dựng một tầng phân giải chung. Ví dụ:

- Số điện thoại quốc tế có cấu trúc khác nhau theo từng quốc gia, nhưng có thể hoạt động toàn cầu nhờ hệ thống mã quốc gia.
- DNS có thể giúp các công nghệ IoT khác nhau tương tác mà không cần thay đổi quy tắc đặt tên hiện tại.

Điều này đã được thực hiện giữa các công nghệ riêng lẻ, giúp chúng tương tác với nhau thông qua DNS, mở ra một phương án khả thi cho việc quản lý định danh IoT trong tương lai.

2.1.3. DNS trong bảo mật IoT

IoT đặt ra nhiều rủi ro bảo mật nghiêm trọng cho cả người dùng và tổ chức, doanh nghiệp, các mối đe dọa bảo mật trong môi trường IoT rất đa dạng, các cơ chế bảo mật hiện có trong IoT vẫn chưa đủ mạnh và thường mang tính đặc thù riêng, vì mỗi nhà cung cấp IoT tự phát triển giải pháp bảo mật khép kín của riêng mình. Điều này trái ngược hoàn toàn với mô hình bảo mật được tiêu chuẩn hóa trên Internet.

Việc truyền dữ liệu trong môi trường IoT thường cần một cổng giao tiếp (gateway) để chuyển đổi giao thức giữa thiết bị IoT (ví dụ: cảm biến sử dụng Bluetooth hoặc LoRa) và các hệ thống mạng lõi trên Internet (ví dụ: hạ tầng Cloud sử dụng giao thức HTTP thông qua địa chỉ IP). Một trong những yêu cầu quan trọng nhất của IoT là kiểm soát điều kiện mà một thiết bị IoT được phép tham gia vào hệ thống Internet.

Tương tự như cách các thiết bị kết nối vào mạng Internet hiện nay, các thiết bị IoT cũng cần phải xác thực trước khi được kết nối. Các thiết bị này cần một định danh (identifier) và một mã xác thực (authentication token) để được chấp nhận trong hệ thống mạng. Tuy nhiên, các công nghệ IoT hiện nay sử dụng các cơ chế xác thực khác nhau, không đồng nhất, do đó phần lớn không tương thích với nhau. Điều này vừa làm giảm tính bảo mật, vừa làm trầm trọng thêm vấn đề tương thích giữa các hệ thống IoT khác nhau.

DNS đã được sử dụng để tăng cường bảo mật trong một số khía cạnh của IoT, đặc biệt là trong việc xác thực thiết bị mới tham gia mạng Internet và bảo vệ quá trình giao tiếp sau đó.

Các nghiên cứu về bảo mật IoT bằng DNS:

- Trong công trình nghiên cứu [Design and implementation of an open LoRaWAN roaming architecture][17] đã đề xuất một hạ tầng khóa công khai (PKI - Public Key Infrastructure) dựa trên DNS để hỗ trợ xác thực thiết bị IoT khi tham gia mạng.
- Trong công trình nghiên cứu [Secure DNS name autoconfiguration for IPv6 internet-of-things devices][18] xây dựng một mô hình Secure Domain Name System Name Autoconfiguration (SDNSNA) cho các thiết bị IoT sử dụng IPv6, dựa trên DNSNA và xác thực NFC (Near Field Communication). Mô hình này cho phép người dùng xác thực và đăng ký thiết bị IoT bằng cách sử dụng điện thoại thông minh, vốn có thể giao tiếp với thiết bị IoT thông qua NFC.
- Trong công trình nghiên cứu [Advanced Secure DNS Name Autoconfiguration with Authentication for Enterprise IoT Network][19] đã giới thiệu phương pháp Advanced Secure DNS Name Autoconfiguration with Authentication and Authorization (ASDAI) dành cho các mạng IoT trong doanh nghiệp, nhằm cải thiện tự động cấu hình DNS với xác thực và cấp quyền bảo mật.
- Trong công trình nghiên cứu [Tracking intruders in IoT networks by means of DNS traffic analysis][20] mở rộng Electronic Product Code Object Name Service (EPC ONS) dựa trên DNS để hỗ trợ nhận dạng đối tượng không đồng nhất một cách linh hoạt.

Ngoài ra, DNS cũng được sử dụng để phát hiện và ngăn chặn các thiết bị IoT độc hại:

- Thiết kế một bộ định tuyến IoT có khả năng phân tích lưu lượng DNS để phát hiện thiết bị IoT kết nối đến các máy chủ DNS không xác định. Điều này rất quan trọng vì các thiết bị IoT bị nhiễm mã độc (botnet) thường sử dụng DNS để kết nối với máy chủ điều khiển (Command-and-Control - C&C).

[17] 130.Balakrichenan S., Bernard A., Marot M., Ampeau B. IoTRoam: Design and implementation of an open LoRaWAN roaming architecture; Proceedings of the IEEE Global Communications Conference (GLOBECOM); Madrid, Spain. 7–11 December 2021. [Google Scholar]

[18] 131.Lee K., Kang H., Jeong J.P., Kim H., Park J.S. Secure DNS name autoconfiguration for IPv6 internet-of-things devices; Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC); Jeju Island, Republic of Korea. 19–21 October 2016; pp. 564–569. [DOI] [Google Scholar]

[19] 132.Kim T.H., Reeves D., Dutta R. Advanced Secure DNS Name Autoconfiguration with Authentication for Enterprise IoT Network; Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM); Madrid, Spain. 7–11 December 2021; pp. 1–6. [DOI] [Google Scholar]

[20] 133.von Sperling T.L., de Caldas Filho F.L., de Sousa R.T., e Martins L.M.C., Rocha R.L. Tracking intruders in IoT networks by means of DNS traffic analysis; Proceedings of the 2017 Workshop on Communication Networks and Power Systems (WCNPS); Brasília, Brazil. 16–17 November 2017; pp. 1–4. [DOI] [Google Scholar]

- DNS Filtering & Extraction Network System (D-FENS) được đề xuất như một hệ thống lọc DNS và phát hiện tên miền độc hại bằng mô hình học sâu (deep learning). D-FENS nằm giữa máy khách DNS và bộ phân giải đệ quy DNS, tiếp nhận các yêu cầu DNS và phát hiện, chặn các miền độc hại mà thiết bị IoT có thể kết nối.

Nhiều giao thức và tiện ích mở rộng đã được phát triển để cải thiện bảo mật của DNS, như đã thảo luận trong các phần trước. Những công nghệ này có thể mang lại lợi ích cho IoT, bao gồm:

- Bảo mật dữ liệu (Security): Ngăn chặn giả mạo DNS, tấn công trung gian (MITM), và truy vấn độc hại.
- Bảo vệ quyền riêng tư (Privacy): Ngăn chặn theo dõi và rò rỉ thông tin từ truy vấn DNS.
- Xác thực (Authentication): Hỗ trợ xác thực thiết bị IoT khi tham gia mạng một cách an toàn.

Hơn nữa, như đã đề cập trước đó, DNS không còn chỉ là một công cụ ánh xạ địa chỉ IP với tên miền. Nhờ các tiện ích mở rộng bảo mật, DNS đang dần trở thành một nền tảng đáng tin cậy để hỗ trợ IoT, từ việc xác thực thiết bị cho đến bảo vệ dữ liệu và quyền riêng tư.

2.1.4. DNS trong vấn đề tương thích của IoT

Hạ tầng IoT cần tích hợp nhiều công nghệ kết nối khác nhau, bao gồm phần cứng, phần mềm, cơ chế định danh, bảo mật, quyền riêng tư và các dịch vụ phân giải tên. Các thành phần này đến từ nhiều bên liên quan khác nhau, khiến khả năng tương thích giữa các hệ thống (interoperability) trở thành yếu tố then chốt trong một mạng IoT hiệu quả. Trong môi trường đa công nghệ, tính tương thích cho phép các thiết bị và hệ thống khác nhau giao tiếp liền mạch, bất kể chúng sử dụng công nghệ hay tiêu chuẩn nào. Điều này bao gồm khả năng trao đổi, sử dụng dữ liệu, dịch vụ và chức năng giữa các hệ thống khác nhau. Tuy nhiên, thiếu tính tương thích là một trong những nhược điểm lớn nhất của IoT hiện nay.

Việc thiếu khả năng tương thích giữa các công nghệ IoT đã khiến hệ sinh thái IoT bị phân mảnh thành nhiều hệ thống không tương thích với nhau. Các công nghệ này phát triển các giải pháp độc quyền và sử dụng các giao thức truyền thông, phương pháp biểu diễn dữ liệu mà ít công nghệ khác có thể hiểu được. Hệ quả là các thiết bị IoT thường chỉ có thể giao tiếp với các thiết bị cùng hệ sinh thái, biến IoT thành những "hòn đảo" biệt lập, mỗi hệ thống hoạt động theo tiêu chuẩn riêng của mình.

DNS đóng vai trò quan trọng trong khả năng tương thích giữa các công nghệ IoT. DNS cung cấp một cách đáng tin cậy để ánh xạ tên thiết bị IoT với địa chỉ mạng hoặc thông tin liên quan đến thiết bị đó. Nhờ có DNS, các công nghệ IoT khác nhau có thể:

- Hợp nhất cơ chế đặt tên, sử dụng DNS như một hệ thống định danh chung
- Tích hợp các dịch vụ dựa trên DNS, cho phép các thiết bị thuộc nhiều hệ sinh thái IoT khác nhau có thể giao tiếp với nhau.

Điều này sẽ giúp xây dựng một hệ sinh thái Web of Things (WoT) liên kết với nhau, với các cơ sở dữ liệu phân tán chứa thông tin về thiết bị IoT và các dịch vụ của chúng. Ngoài ra, DNS hỗ trợ các bản cập nhật động (Dynamic Updates), cho phép tự động cấu hình lại địa chỉ thiết bị, làm cho nó trở thành một giải pháp lý tưởng cho các môi trường IoT động và thay đổi liên tục.

2.1.5. Tác động của IoT đối với hệ thống DNS

Cho đến nay, rất khuyến khích sử dụng DNS để giải quyết nhiều thách thức trong môi trường IoT, đồng thời trình bày cách DNS có thể giảm thiểu các vấn đề đó. Tuy nhiên, cũng cần lưu ý rằng DNS là một trong những nền tảng quan trọng của Internet. Tầm quan trọng của DNS đòi hỏi sự thận trọng khi tích hợp hệ thống này vào IoT, bởi vì quy mô khổng lồ của thiết bị IoT và tài nguyên hạn chế (tính năng bảo mật, tài nguyên phần cứng, phần mềm, ...) có thể gây nguy hiểm cho hệ thống DNS.

Hầu hết các nhà sản xuất IoT ít chú ý đến bảo mật thiết bị. Các thiết bị này thường được thiết kế để thực hiện chức năng cụ thể mà không được trang bị các biện pháp bảo mật đảm bảo an toàn. Ngoài ra, do bị hạn chế tài nguyên, các thiết bị IoT không thể triển khai các giải pháp bảo mật tiên tiến như trên Internet thông thường. Dưới đây là những thách thức mà DNS phải đối mặt khi tích hợp với IoT:

- Trong công trình nghiên cứu [DNS and the Internet of Thing][21] đã chỉ ra những vấn đề về chức năng, bảo mật và khả năng hoạt động của DNS trong môi trường IoT. Trong khi đó, công trình nghiên cứu [Is DNS Ready for Ubiquitous Internet of Things?][22] đã đặt vấn đề và xem xét liệu DNS hiện tại có sẵn sàng hỗ trợ IoT hay không, và đưa ra các tiêu chí cần đáp ứng trước khi sử dụng DNS với IoT về tính bảo mật, hiệu suất, tính linh hoạt,...

Mặc dù việc sử dụng DNS với IoT mang lại nhiều lợi ích, nhưng nếu không được triển khai cẩn thận, nó có thể gây rủi ro nghiêm trọng cho hệ thống DNS toàn cầu.

[21] Hamzic A., Olofsson I. Master's Thesis. KTH Royal Institute of Technology; Stockholm, Sweden: 2016. DNS and the Internet of Things: Outlining the Challenges Faced by DNS in the Internet of Things.

[22] Yan, Z.; Li, H.; Zeadally, S.; Zeng, Y.; Geng, G. Is DNS Ready for Ubiquitous Internet of Things? IEEE Access 2019, 7, 28835–28846.

[23] 15.Aucklah K., Mungur A., Armoogum S., Pudaruth S. The Impact of Internet of Things on the Domain Name System; Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS); Madurai, India. 6–8 May 2021; pp. 449–454. [DOI] [Google Scholar]

2.1.6. Những rủi ro của việc sử dụng DNS với IoT

(1) Các cuộc tấn công DDoS sử dụng IoT

- Số lượng lớn thiết bị IoT có lỗ hổng bảo mật khiến chúng trở thành mục tiêu lý tưởng để xây dựng hệ thống botnet phục vụ cho các cuộc tấn công DDoS nhắm vào hạ tầng Internet, bao gồm cả hệ thống DNS với quy mô lớn. (Cuộc tấn công DDoS của botnet Mirai vào nhà cung cấp dịch vụ DNS DYN đã làm gián đoạn hoạt động của nhiều dịch vụ lớn trên Internet, với sức mạnh lên đến 1,2 Tbps).
- Hàng trăm nghìn thiết bị IoT bị kiểm soát bởi hacker khiến các phương pháp chặn lọc truyền thống dựa trên địa chỉ IP trở nên kém hiệu quả. Điều này giúp các cuộc tấn công kéo dài và khó ngăn chặn hơn.

(2) Lỗ hổng bảo mật trong hệ thống DNS

Năm 2021, một lỗ hổng nghiêm trọng được phát hiện trong các giao thức TCP/IP stack phổ biến, được gọi là "Name: Wreck][23]". Lỗ hổng này cho phép kẻ tấn công thực thi mã từ xa hoặc thực hiện tấn công từ chối dịch vụ (DoS) trên các thiết bị IoT và hệ thống DNS liên quan. Các tổ chức và nhà sản xuất thiết bị IoT cần thận trọng trong việc triển khai DNS, đồng thời tăng cường các cơ chế bảo mật để giảm thiểu rủi ro.

Một số biện pháp có thể giúp bảo vệ hệ thống DNS khi tích hợp với IoT bao gồm:

- Tăng cường bảo mật DNS bằng cách triển khai DNSSEC, QNAME Minimization và các giao thức bảo mật như DNS-over-TLS (DoT) hoặc DNS-over-HTTPS (DoH).
- Giới hạn quyền truy cập DNS của thiết bị IoT bằng cách sử dụng các bộ lọc DNS hoặc danh sách chặn (blacklist).
- Giám sát lưu lượng DNS để phát hiện bất thường, chẳng hạn như các thiết bị IoT bị nhiễm mã độc truy vấn các máy chủ DNS đáng ngờ.
- Khuyến khích các nhà sản xuất IoT triển khai các tiêu chuẩn bảo mật mở, giảm thiểu việc phát triển các giải pháp bảo mật độc quyền, không tuân thủ tiêu chuẩn quốc tế và không đảm bảo tính tương thích.

Nhìn chung, việc tích hợp DNS vào hệ sinh thái IoT mang lại nhiều lợi ích, nhưng cũng tiềm ẩn những rủi ro lớn cho hệ thống DNS toàn cầu. Vì vậy, cần có sự cân nhắc kỹ lưỡng và các biện pháp bảo mật phù hợp để bảo vệ hạ tầng DNS khỏi các mối đe dọa ngày càng gia tăng từ các thiết bị IoT.

2.2. DNS và 5G

2.2.1. DNS trong kiến trúc và hoạt động của mạng 5G

Mạng di động thế hệ thứ năm (5G) là bước tiến quan trọng trong ngành công nghệ viễn thông, cung cấp tốc độ kết nối nhanh hơn, độ trễ thấp hơn và hỗ trợ số lượng kết nối khổng lồ. DNS (Domain Name System) đóng vai trò cốt lõi trong việc đảm bảo hiệu suất cao, độ tin cậy và khả năng mở rộng cho các dịch vụ mạng 5G.

Cụ thể, mạng 5G được thiết kế với nhiều công nghệ mới như điện toán biên (Edge Computing), Network Slicing, Cloud-native Infrastructure, tất cả đều phụ thuộc chặt chẽ vào DNS để vận hành hiệu quả:

- Điện toán biên (Edge Computing): DNS được dùng để phân giải và định tuyến người dùng tới máy chủ biên gần nhất, giúp giảm độ trễ, cải thiện tốc độ truy cập cho các ứng dụng nhạy cảm với thời gian như xe tự hành, thực tế ảo, hay trò chơi điện tử trực tuyến.
- Network Slicing: Trong 5G, các mạng ảo riêng biệt (slices) được tạo ra để phục vụ các dịch vụ đặc thù (như y tế, giao thông thông minh). DNS giúp định tuyến linh hoạt để các truy vấn từ thiết bị trong mỗi slice được dẫn tới các dịch vụ hoặc máy chủ thích hợp, đáp ứng nhu cầu đặc thù của từng loại ứng dụng.
- Cơ sở hạ tầng Cloud-native: DNS giúp 5G tích hợp dễ dàng với hạ tầng đám mây thông qua việc quản lý linh hoạt địa chỉ IP, dịch vụ tự động cấu hình (auto-configuration) và tự động phát hiện tài nguyên (auto-discovery) [1][24] [2][25].

2.2.2. Vai trò của DNS trong phân giải và định tuyến mạng 5G

Việc triển khai mạng 5G yêu cầu DNS xử lý số lượng lớn các truy vấn DNS với tốc độ cao, độ tin cậy cao và thời gian phản hồi rất ngắn (dưới 5ms). Để đáp ứng điều này, các nhà cung cấp dịch vụ mạng 5G đã triển khai các giải pháp DNS tiên tiến như:

- Anycast DNS: Giúp giảm độ trễ bằng cách tự động định tuyến các yêu cầu DNS tới máy chủ gần nhất về mặt địa lý.
- GeoDNS: Cho phép DNS tự động điều hướng lưu lượng mạng 5G dựa trên vị trí địa lý của người dùng, cải thiện đáng kể hiệu suất kết nối và trải nghiệm người dùng.
- DNS-over-HTTPS (DoH) và DNS-over-TLS (DoT): Bảo mật truy vấn DNS khỏi bị nghe lén, giả mạo, giúp nâng cao bảo mật cho người dùng mạng 5G.

[24] "DNS at the Core of 5G Networks," Infoblox white paper, 2022

[25] GSMA Intelligence, "5G Implementation Guidelines"

2.2.3. Ứng dụng DNS trong việc tăng cường bảo mật mạng 5G

Với mạng 5G, bảo mật trở nên đặc biệt quan trọng do phạm vi ứng dụng rộng lớn từ công nghiệp tới hạ tầng quan trọng quốc gia. DNS giúp tăng cường bảo mật mạng 5G thông qua các cơ chế sau:

- DNSSEC (Domain Name System Security Extensions): Đảm bảo tính toàn vẹn và xác thực cho các phản hồi DNS, ngăn chặn tấn công giả mạo DNS (DNS spoofing) và bảo vệ các truy vấn DNS quan trọng trong mạng 5G.
- DNS Firewall và DNS Filtering: Ngăn chặn người dùng và thiết bị mạng 5G kết nối tới các tên miền độc hại, ngăn ngừa các cuộc tấn công botnet, ransomware hay các mối đe dọa khác thông qua DNS.
- Zero Trust DNS: Áp dụng chính sách bảo mật dựa trên định danh và xác thực DNS, đặc biệt quan trọng trong các mạng 5G doanh nghiệp, đảm bảo truy cập an toàn và giám sát chặt chẽ lưu lượng mạng [4][26] [5][27].

2.2.4. Những nghiên cứu về DNS trong mạng 5G

Một số nghiên cứu khoa học gần đây đã nhấn mạnh vai trò then chốt của DNS trong mạng 5G, đồng thời đề xuất các phương pháp cải tiến DNS:

- Trong công trình nghiên cứu về "Optimizing DNS Response in 5G Networks Using SDN"[28] tập trung vào tối ưu hóa DNS trong 5G bằng cách sử dụng mạng định nghĩa bằng phần mềm (SDN - Software-Defined Networking) để tăng cường khả năng phản hồi nhanh, linh hoạt và tự động cấu hình địa chỉ cho thiết bị đầu cuối.
- Trong công trình nghiên cứu về "SmartDNS: Dynamic DNS Resolution for 5G"[29] đề xuất giải pháp DNS thông minh (SmartDNS) giúp mạng 5G có thể thích ứng nhanh với thay đổi về cấu hình mạng, định tuyến tự động và linh hoạt để đáp ứng tốt hơn nhu cầu người dùng.
- Trong công trình nghiên cứu về "AI-driven DNS traffic analytics for security in 5G"[30] sử dụng trí tuệ nhân tạo (AI) để phân tích lưu lượng DNS nhằm dự đoán và phát hiện sớm các tấn công mạng trong môi trường 5G, từ đó tăng cường bảo mật tổng thể cho hệ thống mạng.

2.2.5. Thách thức và giải pháp khi triển khai DNS trong mạng 5G

Dù DNS mang lại nhiều lợi ích trong mạng 5G, nhưng vẫn đối mặt với một số thách thức:

- Hiệu suất và độ trễ: Số lượng truy vấn DNS cực lớn trong mạng 5G đòi hỏi DNS phải phân giải rất nhanh, với thời gian phản hồi tối đa vài mili giây. Các giải pháp như Anycast DNS và DNS caching tại biên đang được triển khai để giảm tải và tăng tốc độ phản hồi.
- Bảo mật và khả năng phục hồi: DNS cần chịu được các cuộc tấn công DDoS quy mô lớn. Các nhà cung cấp DNS trong mạng 5G phải sử dụng công nghệ Anycast, DNS Firewall, DNSSEC và các giải pháp bảo mật tiên tiến khác để giảm thiểu rủi ro.
- Khả năng mở rộng và tự động hóa: DNS trong mạng 5G cần có khả năng mở rộng linh hoạt và hỗ trợ cấu hình tự động. Giải pháp DNS động (Dynamic DNS) và tích hợp với SDN, AI để tối ưu hóa tự động hóa cấu hình, giảm thiểu lỗi do con người là những hướng đi tiềm năng.

2.2.6. Xu hướng phát triển DNS trong mạng 5G tương lai

Tương lai của DNS trong mạng 5G có thể sẽ tập trung vào một số hướng phát triển công nghệ như sau:

- Tích hợp sâu với AI và Machine Learning: DNS trong mạng 5G sẽ sử dụng AI để tự động phát hiện và ứng phó với các mối đe dọa bảo mật, tối ưu hóa hiệu suất DNS theo thời gian thực.
- DNS cho mạng 5G phi tập trung (Decentralized DNS): Sử dụng công nghệ blockchain và DLT (Distributed Ledger Technology) để tăng cường bảo mật, tính minh bạch, độ tin cậy trong việc quản lý và định tuyến DNS cho các mạng 5G.
- Post-Quantum DNS: Nghiên cứu và triển khai các thuật toán mật mã hậu lượng tử (post-quantum cryptography) trong DNSSEC để đảm bảo DNS vẫn an toàn trước nguy cơ máy tính lượng tử trong tương lai.

[26] Akamai, "DNS Security and Zero Trust for 5G"

[27] Ericsson, "Securing 5G Networks"

[28] IEEE Transactions, "Optimizing DNS Response in 5G Networks Using SDN," 2021.

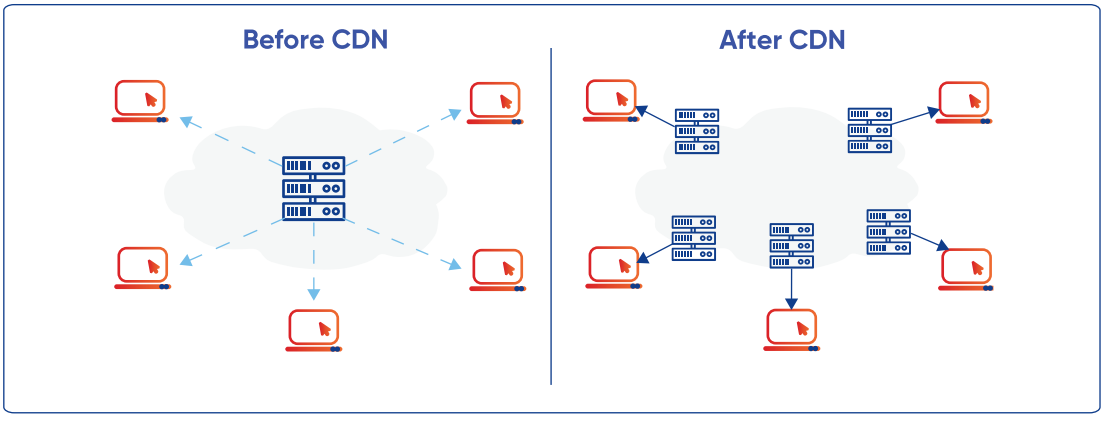
[29] Elsevier, "SmartDNS: Dynamic DNS Resolution for 5G," Computer Networks Journal, 2022.

[30] IEEE Communications, "AI-driven DNS traffic analytics for security in 5G," 2023.

3. DNS và CDN

3.1. CDN là gì

Định nghĩa và cách hoạt động của CDN: CDN (Content Delivery Network) là giải pháp mạng phân phối nội dung, giúp tối ưu hóa việc truyền tải dữ liệu. Mạng phân phối nội dung (CDN) gồm các máy chủ (web, ứng dụng, media,...) có nội dung giống nhau được đặt tại nhiều nơi trên khắp thế giới (được gọi là các máy chủ cache hoặc máy chủ replica). Khi người dùng truy cập website, ứng dụng, media,... công nghệ CDN sẽ giúp lựa chọn máy chủ đặt gần người sử dụng nhất để cung cấp dịch vụ một cách nhanh chóng.



Hình 66: Mô hình có CDN và không có CDN

Hiện nay, trong triển khai thực tế, người ta thường kết hợp sử dụng nhiều mạng phân phối nội dung (CDN) của các nhà cung cấp khác nhau cùng lúc (gọi tắt là Multi-CDN) để tối ưu hóa, nâng cao hiệu suất, độ tin cậy và năng lực dự phòng của việc phân phối nội dung trực tuyến.

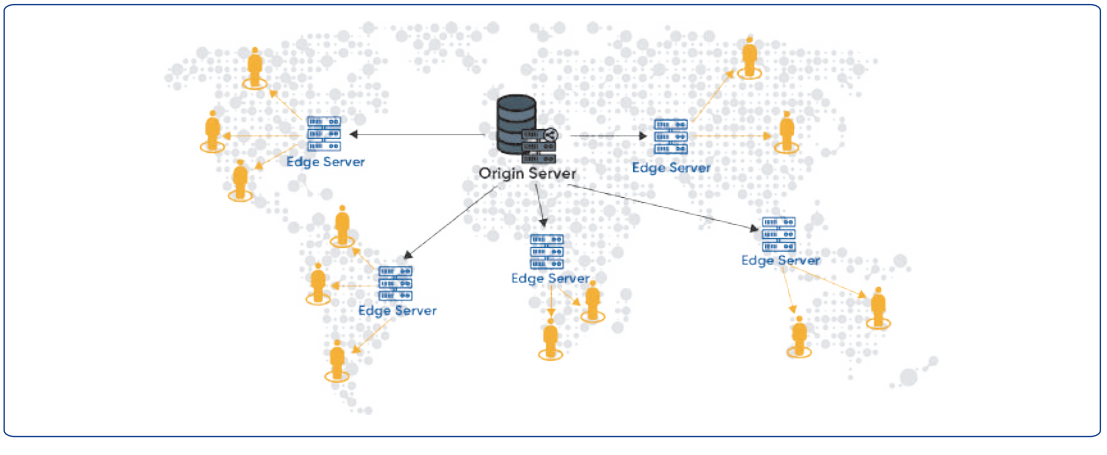
Theo mô hình hoạt động, CDN được chia thành 02 loại như sau:

- Static CDN (Traditional CDN – CDN truyền thống): chủ yếu tập trung vào lưu trữ và phân phối nội dung tĩnh như hình ảnh, video và tập lệnh (scripts) từ máy chủ gốc (Origin server).
- Dynamic CDN: cho phép CDN phân phối cả nội dung tĩnh và động, bao gồm video trực tuyến, website, ứng dụng, truyền thông đa phương tiện và dữ liệu theo thời gian thực, ... phù hợp với các nền tảng như thương mại điện tử, mạng xã hội và trang tin tức.

Ngoài cách phân loại dựa theo mô hình hoạt động, CDN còn có thể được phân loại dựa theo kiến trúc, mục đích, đối tượng sử dụng, ...

Kiến trúc cơ bản của CDN điển hình gồm 02 thành phần chính: máy chủ gốc (Origin server), mạng lưới các máy chủ biên phân tán (gọi là Cache Server/CDN Server/Edge Server):

- Origin Server là thành phần chính của hệ thống, lưu trữ, cung cấp và đồng bộ dữ liệu cho các máy chủ biên phân tán.
- Edge Server là thành phần chịu tải truy cập từ phía người dùng, lưu trữ và truyền tải các dữ liệu tạm thời (cache). Các hệ thống máy chủ biên sẽ được quy hoạch phân bố theo địa lý trên toàn thế giới, quy mô thiết kế dựa trên tính toán lượng truy cập của người sử dụng của các khu vực.



Hình 67: Mô hình kiến trúc CDN

CDN (Content Delivery Network) đóng vai trò quan trọng trong việc quản lý và phân phối dữ liệu trên mạng Internet, đặc biệt trong bối cảnh ngày càng nhiều người dùng truy cập nội dung trực tuyến. Cụ thể:

- Giảm độ trễ, tăng tốc độ truy cập các nội dung trực tuyến và cải thiện trải nghiệm người dùng: CDN giúp phân phối nội dung từ các máy chủ gần người dùng nhất, giúp giảm đáng kể thời gian tải dữ liệu và độ trễ, cải thiện hiệu suất, mang lại trải nghiệm các dịch vụ trực tuyến ổn định và hiệu quả hơn.
- Phân phối nội dung đa phương tiện: CDN hỗ trợ công nghệ adaptive streaming[31], giúp tối ưu hóa phát trực tuyến video theo thời gian thực. Nhờ đó, nội dung video được truyền tải ổn định, không gián đoạn, bất kể loại thiết bị hay chất lượng kết nối mạng. Đây là công nghệ cốt lõi hỗ trợ các nền tảng như Netflix, YouTube, học trực tuyến, cho phép hàng triệu người dùng xem video đồng thời với độ trễ thấp và chất lượng cao.
- Tăng cường bảo mật: CDN không chỉ phân phối nội dung mà các biện pháp bảo mật còn được tích hợp trong CDN bao gồm bảo vệ chống tấn công từ chối dịch vụ phân tán (DDoS protection), mã hóa SSL (Secure Sockets Layer) và tường lửa ứng dụng web (WAF - Web Application Firewall). Những công nghệ này giúp ngăn chặn các cuộc tấn công vào trang web, giảm thiểu nguy cơ rò rỉ dữ liệu, đồng thời tạo dựng lòng tin đối với người dùng trên môi trường Internet.
- Tối ưu hóa băng thông, giúp tiết kiệm chi phí: Nhờ lưu trữ nội dung trên các máy chủ biên (edge server) gần người dùng, CDN giúp giảm đáng kể số lần truy vấn trực tiếp đến máy chủ gốc, từ đó giảm tải dữ liệu, tiết kiệm tài nguyên và tối ưu hóa hiệu suất. Với khối lượng dữ liệu lớn, việc sử dụng CDN không chỉ giúp cắt giảm chi phí băng thông mà còn đảm bảo tốc độ tải nội dung nhanh hơn, nâng cao trải nghiệm người dùng và tối ưu hóa vận hành hệ thống, đặc biệt khả năng mở rộng linh hoạt.
- Tăng cường độ tin cậy và khả năng chịu lỗi cao: CDN tăng cường độ tin cậy và khả năng chịu lỗi cao nhờ kiến trúc phân tán, giúp duy trì dịch vụ ngay cả khi một vài máy chủ biên hoặc trung tâm dữ liệu gặp sự cố. Hệ thống tự động chuyển hướng lưu lượng sang các máy chủ CDN khác để đảm bảo dịch vụ không bị gián đoạn. Ngoài ra có thể sử dụng multi-CDN kết hợp nhiều nhà cung cấp CDN để dự phòng.
- Phân phối nội dung toàn cầu, giúp tiếp cận người dùng quốc tế: CDN giúp phân phối nội dung toàn cầu nhờ mạng lưới máy chủ rộng khắp, cho phép doanh nghiệp phục vụ người dùng quốc tế với hiệu suất, đảm bảo trải nghiệm người dùng nhất quán. Ngoài ra, hệ thống định tuyến động, giúp chuyển hướng lưu lượng khi có sự cố mạng, tăng cường khả năng phục hồi và ổn định dịch vụ.

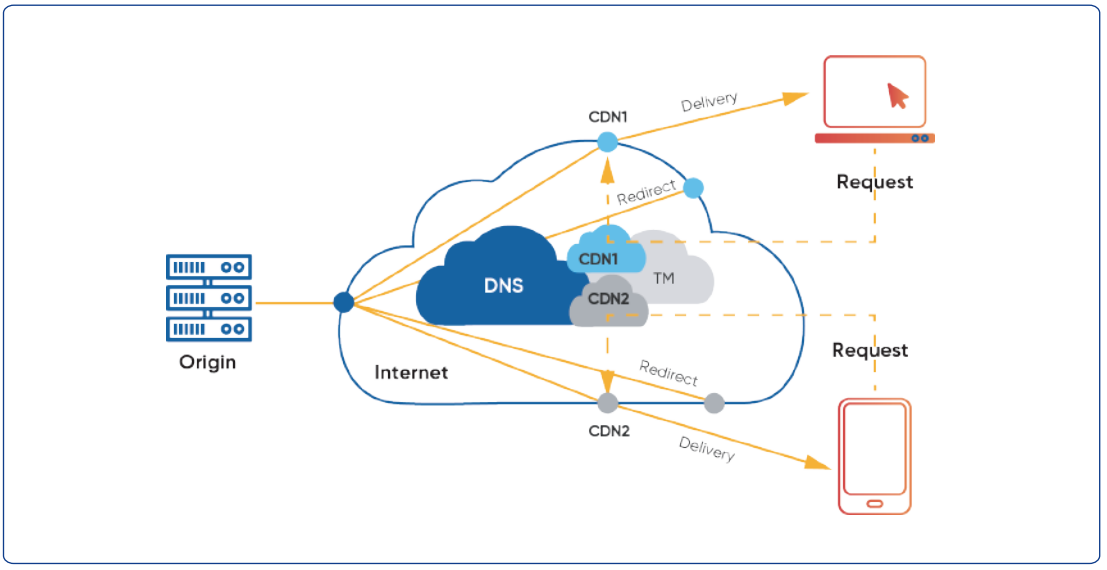
Nếu không có CDN, người dùng kết nối trực tiếp đến máy chủ gốc, mất nhiều thời gian hơn do khoảng cách xa và thiếu tối ưu hóa mạng, đặc biệt trong kỷ nguyên số, nơi mà các dịch vụ, ứng dụng và dữ liệu được truyền tải, chia sẻ và tương tác liên tục trên Internet. Khi lưu lượng truy cập tăng đột biến, hệ thống dễ bị quá tải, gây tắc nghẽn mạng, giảm tốc độ tải trang, tăng độ trễ và ảnh hưởng đến trải nghiệm người dùng. Điều này đặc biệt quan trọng đối với các nền tảng thương mại điện tử, streaming, trò chơi trực tuyến và dịch vụ đám mây, nơi mỗi giây chậm trễ có thể dẫn đến tổn thất doanh thu, giảm lòng tin khách hàng và suy giảm hiệu suất hệ thống. Ngoài ra, việc không có CDN cũng làm gia tăng nguy cơ bảo mật, dễ bị tấn công DDoS và gặp phải các sự cố hạ tầng mạng nghiêm trọng.

3.2. Mối quan hệ giữa CDN và DNS

DNS là thành phần bắt buộc, không thể thiếu khi triển khai CDN. Thông thường, khi truy cập tên miền, DNS sẽ trả về địa chỉ IP của máy chủ gốc, tuy nhiên trong hệ thống CDN, DNS có thể trả về địa chỉ IP của một máy chủ CDN gần người dùng nhất. Sau khi DNS trả về IP của máy chủ CDN phù hợp, người dùng sẽ kết nối đến máy chủ đó và yêu cầu tài nguyên (ví dụ: hình ảnh, video, CSS, JavaScript).

- Nếu nội dung đã được lưu trữ trên máy chủ CDN (cache), máy chủ CDN sẽ trả về tài nguyên ngay lập tức mà không cần yêu cầu lại từ máy chủ gốc, giúp giảm độ trễ và tăng tốc độ tải.
- Nếu tài nguyên chưa có trên máy chủ CDN (lần đầu tiên yêu cầu), máy chủ CDN sẽ lấy dữ liệu từ máy chủ gốc và lưu trữ tạm thời (cache). Sau đó, nó sẽ phục vụ tài nguyên này cho các yêu cầu tiếp theo từ người dùng.

[31] Công nghệ adaptive streaming tự động điều chỉnh chất lượng video dựa trên băng thông mạng, hiệu suất thiết bị và điều kiện kết nối của người dùng



Hình 68: DNS và CDN

DNS giữ vai trò then chốt trong việc định hướng người dùng đến đúng máy chủ CDN. Như đã đề cập, CDN sử dụng DNS để quyết định máy chủ biên nào sẽ phục vụ yêu cầu của người dùng. Nhà cung cấp CDN gán một tên miền CDN cho nội dung của khách hàng; khi người dùng truy cập, truy vấn DNS sẽ được xử lý bởi hệ thống DNS của CDN. Dựa trên vị trí truy vấn (thường là vị trí của DNS resolver của ISP người dùng), máy chủ DNS của CDN sẽ trả về địa chỉ IP của máy chủ biên tối ưu (gần nhất hoặc tải thấp nhất) cho người dùng. Toàn bộ quá trình này diễn ra trong vài chục mili-giây, giúp tự động phân phối tải và định tuyến lưu lượng người dùng đến vị trí tối ưu.

Ngoài ra, DNS còn được dùng trong các mô hình giải pháp multi-CDN, nơi một lớp DNS thông minh đóng vai trò phân giải tên miền sang các CDN khác nhau tùy theo tình hình (ví dụ: CDN A gặp lỗi thì DNS trỏ sang CDN B). Tóm lại, DNS là "hệ thống dẫn đường" không thể thiếu để CDN vận hành hiệu quả trên phạm vi toàn cầu. Có hai cơ chế phổ biến để CDN dùng DNS chuyển hướng người dùng:

- Dùng các bản ghi DNS động theo khu vực (GeoDNS): DNS của CDN sẽ dựa trên vị trí địa lý của truy vấn (thông qua IP của client hoặc của resolver) để trả về một câu trả lời khác nhau cho từng vùng, khu vực – ví dụ người dùng từ Việt Nam nhận IP của máy chủ biên ở khu vực Đông Nam Á, người dùng châu Âu nhận IP máy chủ biên ở khu vực EU.
- Dùng Anycast IP: CDN có thể dùng một địa chỉ IP chung cho toàn bộ hệ thống, quảng bá địa chỉ đó trên nhiều PoP khác nhau; lúc này DNS chỉ trả về một IP duy nhất cho mọi người dùng, nhưng giao thức định tuyến Anycast của Internet sẽ tự động hướng mỗi người dùng tới "phiên bản" máy chủ biên gần nhất mang IP đó. Dù theo cách nào, DNS vẫn là điểm mấu chốt khởi đầu để quyết định người dùng được phục vụ bởi máy chủ nào trong mạng CDN.

3.3. Cách CDN sử dụng DNS để tối ưu hóa nội dung

CDN không chỉ dựa vào DNS thông thường, mà còn triển khai nhiều kỹ thuật DNS nâng cao để tối ưu hiệu quả phân phối: ví dụ GeoDNS để trả lời DNS dựa trên vị trí địa lý của người dùng, DNS Load Balancing để phân tải giữa các máy chủ, Anycast DNS để tăng tốc phân giải và CNAME Flattening/ALIAS để khắc phục hạn chế kỹ thuật khi trỏ tên miền gốc vào CDN. Chúng ta sẽ lần lượt tìm hiểu các công nghệ này ở phần sau đây:

3.3.1. GeoDNS (DNS dựa trên vị trí địa lý)

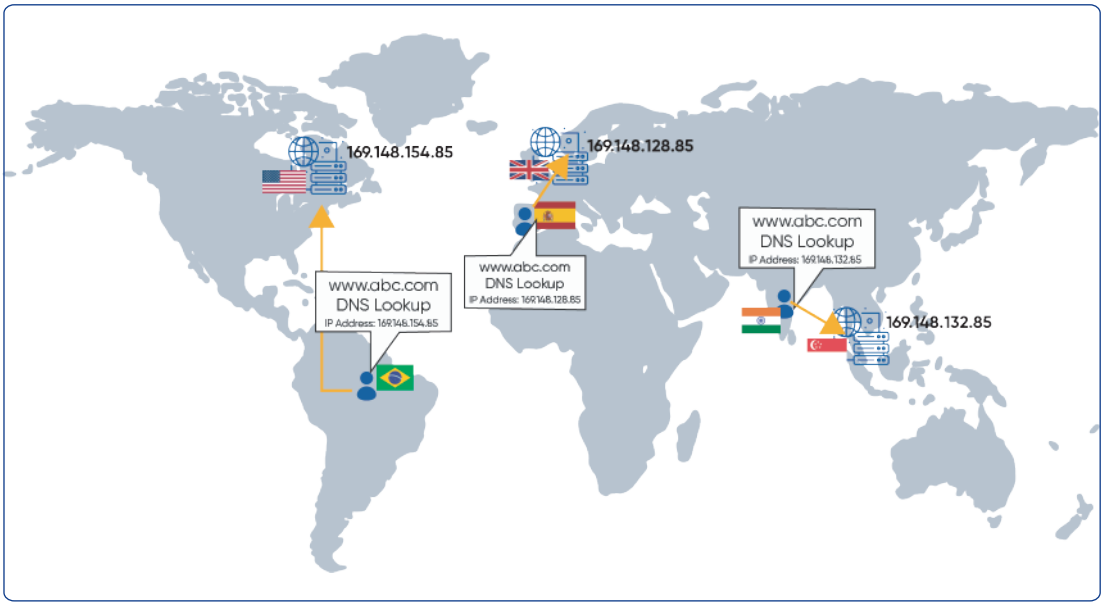
GeoDNS là kỹ thuật phân giải DNS trong đó câu trả lời DNS phụ thuộc vào vị trí địa lý của người truy vấn, với mục đích là xác định máy chủ DNS ở gần người người dùng nhất về mặt địa lý nhằm giảm thiểu độ trễ của phản hồi truy vấn.

Cơ chế hoạt động như sau: khi một DNS resolver của người dùng gửi truy vấn tên miền, máy chủ DNS (authoritative) sẽ xác định vị trí người dùng dựa trên địa chỉ IP nguồn của truy vấn (thường là IP của resolver) và trả về địa chỉ IP của máy chủ (hoặc node CDN) phù hợp với khu vực đó. Ví dụ, cùng một tên miền www.vnnic.vn nhưng người dùng ở châu Âu có thể nhận được IP của máy chủ đặt tại Đức, trong khi người dùng ở châu Á nhận IP của máy chủ ở Singapore. Hệ thống GeoDNS giữ một cơ sở dữ liệu địa lý (GeoIP) để ánh xạ địa chỉ IP và vị trí (quốc gia, khu vực) và sử dụng nó khi trả lời, phản hồi truy vấn.

GeoDNS được sử dụng rộng rãi trong các mạng CDN và dịch vụ toàn cầu. Nó hoạt động như một "bộ cân bằng tải địa lý": phân tán người dùng khắp thế giới về các cụm máy chủ gần người dùng nhất, tránh tình trạng lưu lượng truy cập của tất cả người dùng dồn về một nơi hoặc phân phối không hợp lý. Ngoài ra, GeoDNS còn giúp định tuyến nhằm tránh các khu vực, đang xảy ra sự cố mạng – ví dụ nếu máy chủ khu vực Bắc Mỹ đang quá tải hoặc gặp lỗi, DNS có thể tạm thời trả về IP máy chủ ở khu vực khác (gần đó) để đảm bảo dịch vụ liên tục.

Tuy nhiên, GeoDNS còn có một số điểm hạn chế, do thường dựa vào IP của DNS resolver (người dùng thường dùng DNS của ISP hoặc các nhà cung cấp dịch vụ Public DNS như: Google Public DNS, Cloudflare, Quad9, ...). Nếu resolver không nằm cùng khu vực với người dùng, việc xác định vị trí có thể không đảm bảo độ chính xác cao. Để khắc phục vấn đề trên, tiêu chuẩn mở rộng EDNS0 Client Subnet (EDNS ECS) ra đời cho phép resolver gửi thông tin dải IP của client lên cho Authoritative DNS Server. Khi Authoritative DNS Server nhận được thông tin subnet của client, nó sẽ dựa trên đó để xác định vị trí người dùng thực sự chính xác hơn. Nhờ EDNS Client Subnet, GeoDNS có thể hoạt động hiệu quả ngay cả khi người dùng dùng resolver ở khoảng cách xa (ví dụ người dùng Việt Nam dùng Google DNS 8.8.8.8 đặt tại Singapore vẫn có ECS chứa IP Việt Nam, Authoritative DNS Server biết và trả về máy chủ biên tại Việt Nam thay vì Singapore). Hiện nay, các DNS của Cloudflare, Google, ... đều hỗ trợ EDNS ECS, giúp các CDN và dịch vụ GeoDNS tăng độ chính xác trong phân phối.

Hình dưới đây minh họa cho hoạt động của GeoDNS: người dùng từ các quốc gia như Brazil, Anh, Ấn Độ gửi truy vấn DNS với tên miền www.abc.com, và mỗi người nhận được một IP khác nhau trỏ tới máy chủ ở từng khu vực (Mỹ, châu Âu, châu Á) – nhờ đó họ sẽ kết nối web tới máy chủ vùng mình thay vì sang lục địa khác.



Hình 69: Minh hoạt hoạt động của GeoDNS

3.3.2. DNS Load Balancing (Phân tải DNS)

Bên cạnh yếu tố địa lý, DNS còn được sử dụng để cân bằng tải giữa nhiều máy chủ hoặc nhiều cụm máy chủ. DNS Load Balancing là kỹ thuật trong đó một tên miền được cấu hình trỏ tới nhiều địa chỉ IP và hệ thống DNS sẽ luân phiên hoặc tùy chọn trả về các IP khác nhau giữa mỗi lần truy vấn, hoặc trả về danh sách IP để client thực hiện truy vấn lần lượt. Cách đơn giản nhất là Round-robin DNS – ví dụ chúng ta có 3 máy chủ cho api.vnnic.vn, chúng ta tạo 3 bản ghi A trỏ cùng tên miền đó đó tới 3 IP khác nhau. Mỗi lần nhận truy vấn, DNS có thể xáo trộn thứ tự các bản ghi hoặc xoay vòng IP trả lời, giúp phân tán các kết nối người dùng vào 3 máy chủ (chia tải lưu lượng truy vấn). Phương pháp đơn giản này giúp chia đều tải nhưng không thể tính toán và xác định được tính khả dụng của các máy chủ đó.

Các CDN và nhà cung cấp DNS với tính năng nâng cao thường có "smart" DNS load balancing, nghĩa là có thể dựa trên dữ liệu giám sát để quyết định câu trả lời. Ví dụ, sử dụng các hệ thống theo dõi độ trễ mạng, tải CPU/ RAM và tình trạng sức khỏe của máy chủ, lưu lượng kết nối hiện tại, ... để chọn máy chủ tối ưu nhất tại thời điểm truy vấn chứ không chọn ngẫu nhiên. Kỹ thuật này gọi là Failover DNS, bản chất là cấu hình, khai báo tối thiểu 02 bản ghi địa chỉ IPv4/ IPv6 cho một tên miền, trong đó có một bản ghi chính và một bản ghi dự phòng, trong trường hợp mặc định sẽ luôn trả về IP chính, nhưng sẽ tự động chuyển sang trả về IP dự phòng nếu phát hiện máy chủ chính ngừng phản hồi. Nhờ đó, DNS đóng vai trò điều phối đảm bảo dịch vụ không gián đoạn.

Trong bối cảnh CDN, DNS Load Balancing kết hợp với GeoDNS tạo thành GSLB (Global Server Load Balancing) – cân bằng tải máy chủ toàn cầu. GSLB dùng nhiều tiêu chí (vị trí địa lý, độ trễ, tải hệ thống, băng thông, ...) để chọn ra cụm máy chủ hoặc node CDN tốt nhất cho mỗi người dùng.

Các nhà cung cấp DNS dịch vụ như NS1, Azure Traffic Manager, Cloudflare Load Balancer, ... cung cấp rất nhiều thuật toán DNS load balancing từ round-robin, weighted (phân theo trọng số %), đến geo steering, latency-based routing (định tuyến theo độ trễ đo thực tế), geofencing (chia theo vùng cụ thể), v.v. Nhờ đó, doanh nghiệp có thể xây dựng một hệ thống Multi-CDN hoặc Multi-IDC và dùng DNS để "điều tiết lưu lượng" một cách linh hoạt.

DNS Load Balancing giúp phân phối đều và tối ưu tải đến các tài nguyên mạng, đảm bảo không máy chủ nào bị quá tải và tăng tính sẵn sàng.

3.3.3. Anycast DNS cho CDN

Anycast là một kỹ thuật định tuyến trong đó cùng một địa chỉ IP được phát quảng bá (announce) từ nhiều địa điểm khác nhau. Khi một gói tin được gửi tới địa chỉ IP anycast, mạng BGP sẽ tự động hướng gói tin đó đến nút gần nhất (theo tiêu chí định tuyến) trong số các nút có quảng bá IP này. Anycast thường được triển khai cho DNS và CDN để cải thiện hiệu năng và khả dụng.

Anycast DNS được triển khai trên cả các hệ thống máy chủ Authoritative DNS Server và DNS Resolver với các lợi ích mang lại như sau:

- Tăng tốc độ phân giải DNS: thay vì mọi truy vấn đổ về một cụm DNS cố định (có thể xa người dùng), anycast DNS giúp truy vấn được xử lý bởi một server ở gần, giảm độ trễ DNS. Thử nghiệm cho thấy anycast có thể rút ngắn thời gian truy vấn DNS xuống chỉ còn vài ms ở nhiều nơi, so với hàng chục ms nếu truy vấn tới các máy chủ ở các khu vực có khoảng cách xa về vị trí địa lý.
- Tăng tính dự phòng: nhiều node anycast cùng sử dụng chung một IP, nếu một node không khả dụng hoặc mạng đến node đó gặp trục trặc, định tuyến BGP sẽ tự động đẩy truy vấn sang node khác (thông thường người dùng sẽ được chuyển hướng sang cụm khác gần gần tiếp theo).

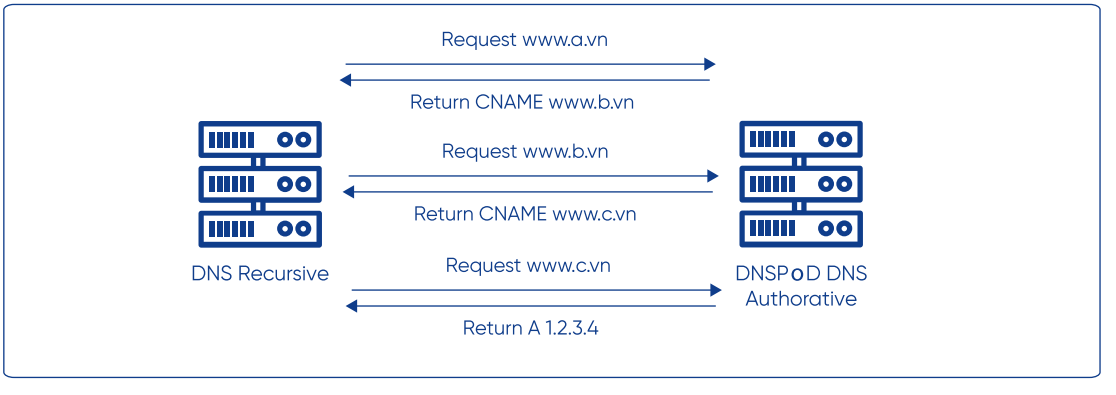
3.3.4. DNS CNAME Flattening & ALIAS Record

Đây là các kỹ thuật DNS giúp đơn giản hóa cấu hình tên miền gốc với CDN, theo quy định trong DNS, tại tên miền gốc (zone apex) của một tên miền (ví dụ vnnic.vn), không được phép tạo CNAME cho chính tên miền gốc đó – bản ghi CNAME chỉ hợp lệ cho các tên miền con (subdomains). Hạn chế này gây khó khăn khi tích hợp CDN, thông thường để trỏ cấu hình, kết nối vào CDN, chúng ta thường dùng CNAME trỏ tới tên miền do CDN cung cấp (ví dụ vnnic.vn.cdn.cloudflare.net), nhưng nếu muốn dùng trực tiếp tên miền gốc (không có www) thì không thể tạo CNAME. Trước đây, giải pháp là buộc dùng một subdomain (ví dụ www.vnnic.vn) để trỏ CNAME đến CDN, rồi thiết lập chuyển hướng từ tên miền chính sang tên miền con được cấu hình sử dụng CDN. Tuy nhiên, điều này không thuận tiện và không tối ưu.

Để khắc phục, các nhà cung cấp DNS đã đưa ra tính năng CNAME Flattening (hay ANAME, ALIAS record – tùy tên gọi của từng nhà cung cấp dịch vụ). Về bản chất, CNAME Flattening cho phép trỏ tên miền gốc (zone apex) tới một tên miền khác.

Cloudflare là hãng tiên phong cung cấp CNAME Flattening từ năm 2014 – cho phép khách hàng trỏ thẳng tên miền gốc tới Cloudflare mà không vi phạm RFC. Khi bật tính năng này, Cloudflare DNS sẽ đóng vai trò recursive resolver để tự phân giải các CNAME và trả về IP cuối cùng cho client. Theo Cloudflare, quá trình flattening[32] này có thể cần một hoặc nhiều truy vấn phía sau, nhưng họ vẫn đảm bảo tốc độ rất nhanh – giúp truy vấn DNS nhanh hơn tới 30% nhờ loại bỏ bước trả CNAME trung gian cho client.

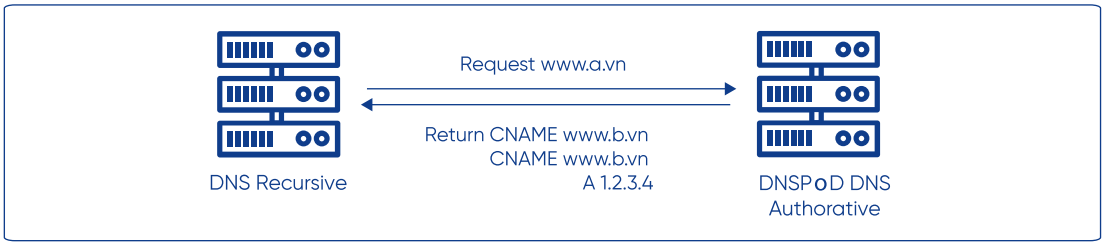
- **Quá trình phân giải trước khi CNAME Flattening:**



Hình 70: Quá trình phân giải trước khi CNAME Flattening

[32] https://developers.cloudflare.com/dns/cname-flattening/

- **Quá trình phân giải sau khi CNAME Flattening:**



Hình 71: Quá trình phân giải sau khi CNAME Flattening

CNAME Flattening/ANAME/ALIAS là các giải pháp DNS sáng tạo để giải quyết vấn đề "tên miền gốc không CNAME được". Áp dụng trong việc tích hợp CDN, dịch vụ cloud vào tên miền gốc trở nên dễ dàng, không còn phải dùng trung gian bằng tên miền con "www" hay vấn đề vi phạm tiêu chuẩn DNS.

3.4. Ứng dụng & Lợi ích của việc kết hợp CDN với DNS

Việc kết hợp CDN với DNS một cách hiệu quả mang lại nhiều lợi ích to lớn cho việc phân phối nội dung trên Internet. Dưới đây là những ứng dụng và lợi ích chính:

- Tăng tốc độ tải nội dung (Improve Load Times): Bằng cách đưa nội dung đến gần người dùng hơn (nhờ CDN) và tăng tốc độ truy cập (nhờ DNS định tuyến thông minh). Điều này cực kỳ quan trọng đối với trải nghiệm của người dùng; Google thống kê rằng 53% người dùng di động sẽ bỏ trang nếu thời gian tải quá 3 giây[33]. Thời gian tải giảm từ 19 giây xuống 5 giây có thể tăng gấp đôi doanh thu quảng cáo trên mobile. Amazon cũng từng phát hiện mỗi 100ms độ trễ tăng thêm làm giảm 1% doanh số bán hàng. Ngược lại, website nhanh hơn đồng nghĩa người dùng ở lại lâu hơn, tương tác nhiều hơn. Việc sử dụng CDN & DNS giúp các trang web đạt tốc độ tối ưu ở mọi nơi.
- Giảm độ trễ và tối ưu hóa trải nghiệm người dùng: Độ trễ (latency) thấp đồng nghĩa với trải nghiệm "mượt" – đặc biệt quan trọng cho các ứng dụng thời gian thực, video trực tuyến, game, hoặc trang web tương tác. CDN kết hợp DNS góp phần giảm độ trễ trên nhiều khía cạnh; độ trễ trong truy vấn và phản hồi truy vấn DNS, độ trễ truyền tải dữ liệu giảm nhờ rút ngắn khoảng cách (mạng lưới các máy chủ CDN đặt gần người dùng) và nhờ các tối ưu mạng của CDN.
- Bảo mật với CDN & DNS (Chống DDoS, bảo vệ dữ liệu): Sự kết hợp CDN và DNS không chỉ tăng tốc mà còn tăng cường bảo mật cho hệ thống, CDN có khả năng chống chịu các cuộc tấn công DDoS quy mô lớn nhờ mạng lưới phân tán và băng thông cao.

CDN giúp bảo vệ dữ liệu và ứng dụng web thông qua các tính năng bảo mật tích hợp: Multi-CDN (Cloudflare, Akamai, ...) cung cấp WAF (Web Application Firewall) chặn các cuộc tấn công ứng dụng (SQL injection, XSS), SSL/TLS encryption miễn phí giúp mã hóa lưu lượng người dùng, và ẩn giấu địa chỉ IP của máy chủ gốc. CDN & DNS cũng hỗ trợ DNSSEC để ngăn chặn giả mạo DNS (DNS spoofing) – đảm bảo bản ghi DNS không bị chỉnh sửa trên đường truyền, người dùng không bị trỏ nhầm sang server giả mạo.

CDN và DNS tạo ra một lớp bảo vệ đa tầng: lớp mạng được củng cố (phân tán, tránh single-point-of-failure, chống DDoS), lớp ứng dụng được bảo vệ (nhờ WAF, ẩn địa chỉ IP gốc), và lớp DNS cũng an toàn hơn (nhờ DNSSEC, Anycast). Điều này cho phép các doanh nghiệp nhỏ cũng có thể phòng chống và giảm thiểu ảnh hưởng của các cuộc tấn công mạng với quy mô lớn.

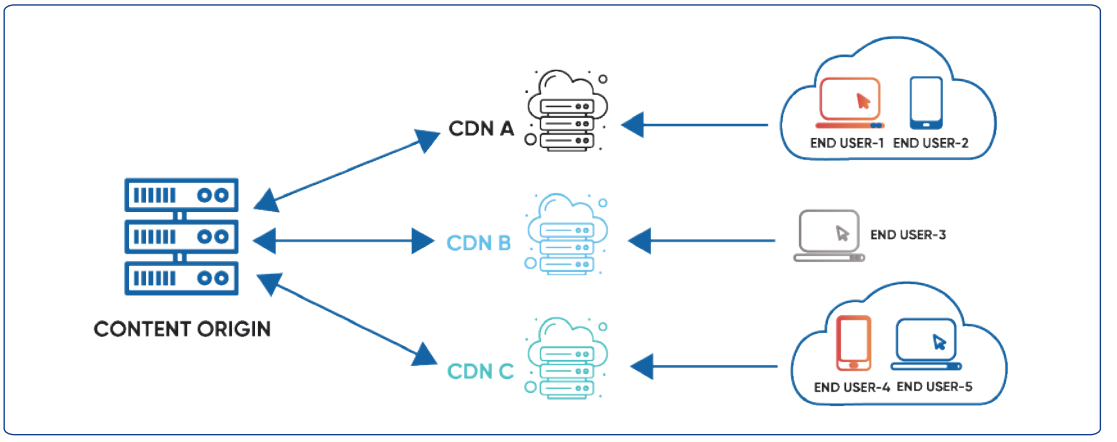
3.5. Các mô hình triển khai CDN & DNS

Có nhiều cách thức để triển khai CDN kết hợp với DNS, tùy thuộc vào nhu cầu, quy mô và nguồn lực của mỗi tổ chức. Dưới đây là một số mô hình phổ biến:

- Triển khai CDN với DNS công cộng của nhà cung cấp dịch vụ: Đây là cách dễ dàng và thường được khuyến nghị cho hầu hết trường hợp. Ở mô hình này, chúng ta sử dụng dịch vụ CDN của một nhà cung cấp (ví dụ Cloudflare, Akamai, Fastly, v.v.) và đồng thời sử dụng dịch vụ DNS (Authoritative DNS Server) của chính các nhà cung cấp dịch vụ CDN đó hoặc tích hợp với một DNS Public khác.
- Sử dụng dịch vụ CDN kết hợp với DNS nội bộ (tự quản lý): Một số tổ chức có nhu cầu quản lý DNS riêng (vì lý do pháp lý, chính sách, hoặc muốn kiểm soát tuyệt đối) nhưng vẫn muốn dùng CDN bên ngoài. Khi đó, mô hình sẽ xây dựng hệ thống DNS riêng do tổ chức tự vận hành (hoặc thuê dịch vụ DNS bên thứ ba không gắn với CDN); đồng thời sử dụng dịch vụ CDN của một nhà cung cấp (Cloudflare, Akamai, Fastly, ...). Ưu điểm của cách này là có thể tự kiểm soát hệ thống DNS (ví dụ một số chính phủ/tổ chức yêu cầu DNS phải nằm trong nước hoặc do chính tổ chức quản lý với các chính sách bảo mật riêng). Tuy nhiên, nhược điểm là sẽ phải tự cấu hình các bản ghi DNS tối ưu cho CDN.

[33] https://www.thinkwithgoogle.com/intl/en-emea/marketing-strategies/app-and-mobile/mobile-page-speed-new-industry-benchmarks/

- Tối ưu hóa DNS khi sử dụng Multi-CDN: Ngày nay, nhiều doanh nghiệp lớn áp dụng chiến lược đa CDN (Multi-CDN) – sử dụng đồng thời từ 2 CDN trở lên.



Hình 72: Multi-CDN

Mục đích là để tối ưu hóa, nâng cao hiệu suất, độ tin cậy và năng lực dự phòng của việc phân phối nội dung trực tuyến. Khi một CDN gặp lỗi, hệ thống có thể tự động chuyển hướng lưu lượng sang một CDN khác, giúp duy trì hiệu suất tối ưu, giảm rủi ro downtime và đảm bảo liên tục hoạt động kinh doanh.

3.6. Xu hướng triển khai tích hợp CDN & DNS

Công nghệ CDN và DNS không ngừng phát triển để đáp ứng nhu cầu ngày càng cao về tốc độ, bảo mật và độ tin cậy trên Internet. Trong tương lai, ta có thể chờ đợi một số xu hướng và tiến bộ sau:

- Sự phát triển của công nghệ CDN và DNS: CDN đang dần phát triển và chuyển từ việc chỉ phân phối nội dung tĩnh sang thành nền tảng phân phối đa nội dung (nội dung động, ứng dụng, trò chơi trực tuyến, ...). Xu hướng Edge Computing kết hợp với CDN cho phép triển khai các ứng dụng, chức năng (serverless functions) ngay tại máy chủ biên giúp giảm độ trễ phản hồi. Các nhà cung cấp CDN như Cloudflare, Fastly, Amazon, ... đã cung cấp khả năng chạy code ở edge. Hệ thống DNS cũng đang được hiện đại hóa, các tiêu chuẩn mới như DNS over HTTPS/TLS/QUIC giúp DNS an toàn hơn. Quy mô DNS anycast ngày càng tăng – các mạng DNS phân tán được mở rộng hơn để áp dụng cho 5G/IoT.
- Ứng dụng AI & Machine Learning trong tối ưu hóa CDN: Trí tuệ nhân tạo được dự báo sẽ đóng vai trò lớn trong việc vận hành CDN tự động và tối ưu hơn nữa. Nhờ AI/ML, CDN có thể phân tích lượng dữ liệu khổng lồ về lưu lượng, hành vi người dùng, hiệu suất mạng theo thời gian thực, từ đó tự đưa ra quyết định điều phối tối ưu vượt quá khả năng các thuật toán tĩnh hiện tại.
- DNS sẽ tiếp tục là "xương sống" cho việc định danh và định tuyến trong môi trường Internet phân tán. Tuy nhiên, DNS cũng đang được cải tiến để phù hợp hơn với kiến trúc hiện đại. Tích hợp sâu hơn giữa DNS và ứng dụng thông qua các bản ghi đặc biệt và giao thức mới. IETF đã tiêu chuẩn hóa bản ghi SVCB/HTTPS – một loại DNS record dùng để cải thiện việc cấu hình và triển khai các dịch vụ HTTPS, đặc biệt là trong việc tối ưu hóa việc truyền tải các dịch vụ web an toàn.
- Tăng cường bảo mật và độ tin cậy: Trong tương lai CDN & DNS ngày càng được tăng cường các giải pháp bảo mật, đặc biệt là các giải pháp như DNSSEC, các tiêu chuẩn mới DoT/DoH hay DoQ sẽ ngày càng được triển khai rộng rãi và bắt buộc.

PHẦN 3

CÁC BÀI THỰC HÀNH

XVI

THỰC HÀNH (LAB)

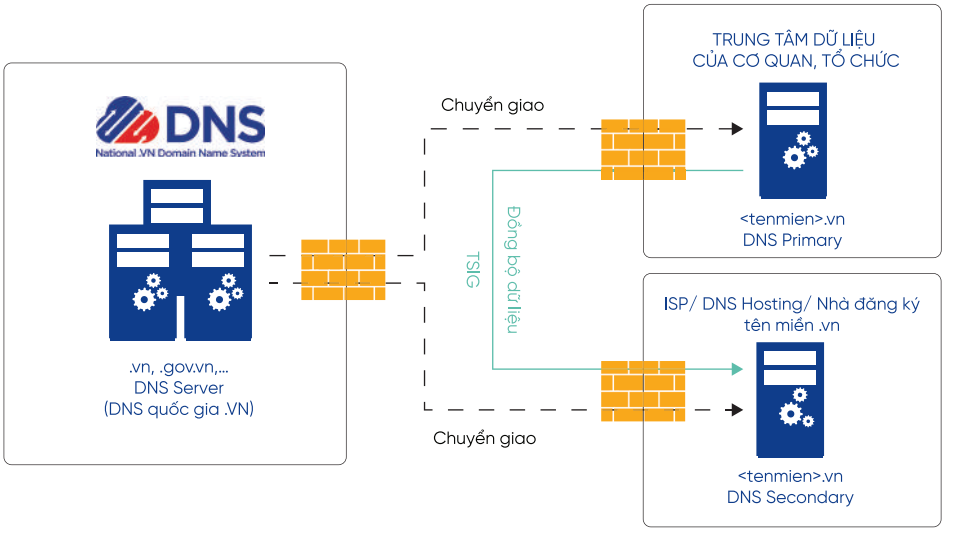
Trong tài liệu này sẽ tập trung hướng dẫn thực hành các bài LAB theo các mô hình triển khai DNS tiêu chuẩn. Việc cài đặt, cấu hình máy chủ DNS sử dụng phần mềm BIND, trên môi trường hệ điều hành Unix/Linux (như CentOS, Ubuntu, Debian, Redhat Linux, ...). Để có thể cài đặt được máy chủ DNS cần có các kiến thức và biết sử dụng được các lệnh trong hệ điều hành Unix/Linux.

1. Mô hình triển khai DNS tiêu chuẩn

Đối với mỗi tổ chức, doanh nghiệp, nhằm đảm bảo tính an toàn an ninh, thông thường sẽ tự xây dựng, triển khai và quản lý, vận hành 02 hệ thống máy chủ DNS thành phần bao gồm: Hệ thống máy chủ DNS quản lý tên miền của chính cơ quan, tổ chức và hệ thống máy chủ tên miền đệm (DNS Caching) nhằm phục vụ người dùng nội bộ. Các hệ thống này đều là thành phần hạ tầng thông tin quan trọng của các cơ quan, tổ chức và được khuyến nghị mô hình triển khai tiêu chuẩn tại Công văn số 273/BTTTT-CBĐTW ngày 31 tháng 01 năm 2020 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ), V/v hướng dẫn mô hình tham chiếu về kết nối mạng cho bộ, ngành, địa phương. Chi tiết các mô hình khuyến nghị tiêu chuẩn như sau:

1.1. Mô hình máy chủ DNS quản lý tên miền

Mô hình tổng thể về DNS quản lý tên miền của cơ quan, tổ chức theo hình vẽ như sau:



Hình 73: Mô hình máy chủ quản lý tên miền

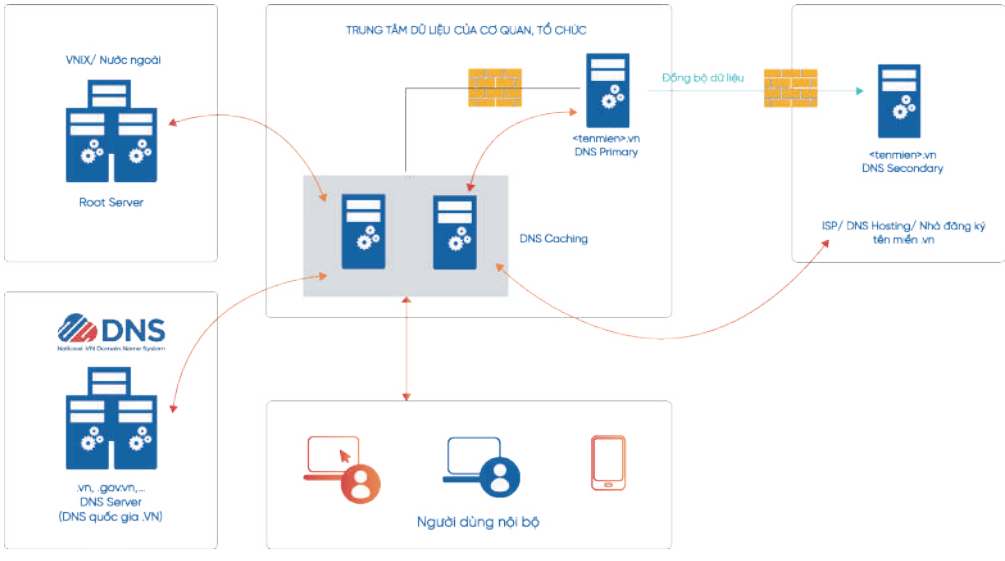
Cơ quan, tổ chức sẽ có tối thiểu 02 máy chủ DNS để quản lý tên miền, máy chủ chính (Master) đặt tại TTDL của chính cơ quan, tổ chức đó (nếu có) hoặc thuê đặt máy chủ tại các IDC, máy chủ phụ (secondary) đặt thuê tại ISP/Đơn vị cung cấp dịch vụ DNS Hosting.

Với các yêu cầu cụ thể như sau:

- Máy chủ DNS: tối thiểu 02 máy chủ DNS với địa chỉ IP khác nhau quản lý tên miền đặt ở 02 mạng độc lập khác nhau: tại TTDL của cơ quan, tổ chức và tại các đơn vị cung cấp dịch vụ như ISP, DNS Hosting hoặc nhà đăng ký tên miền .vn.
- 01 máy chủ DNS Primary (Master) quản lý dữ liệu chính, toàn bộ khai báo các bản ghi dịch vụ như <www, mail, edoc> được thực hiện trên máy chủ này.
- 01-02 máy chủ DNS Secondary (Slave): được đồng bộ với máy chủ master theo cơ chế zone transfer, sử dụng TSIG để đảm bảo an toàn (XFR + TSIG). Cơ chế TSIG (transaction signature) là quá trình sử dụng chung mã bảo mật chia sẻ giữa máy chủ DNS Primary và DNS Secondary để đảm bảo giao tiếp giữa các máy chủ DNS được xác thực.

- Ghi nhật ký hoạt động, phần mềm giám sát DNS, phân tích log DNS.
- Triển khai DNSSEC, đóng vai trò ký DNSSEC cho tên miền để đảm bảo an toàn tên miền. Các công việc thực hiện sẽ là tạo ra các khóa DNSSEC và ký lên zone tên miền <tenmien>.vn. Gửi cập nhật đăng ký bản ghi chuyển giao (Deligation Signer - DS) lên hệ thống DNS quốc gia do VNNIC quản lý thông qua các nhà đăng ký tên miền .vn.
- Triển khai máy chủ DNS chạy song song IPv4, IPv6 (dual-stack).
- Khai báo các bản ghi AAAA cho các tên miền như <www, mail, edoc> để hoạt động được trên mạng Internet IPv6.
- Thiết lập chính sách tường lửa (firewall): UDP-53, TCP-53 (truy vấn DNS); cho phép truy vấn EDNS(0) (truy vấn DNS hỗ trợ IPv6, DNSSEC).
- Các phần mềm tham khảo: BIND 9.x, NSD, PowerDNS, Knot,...

1.2. Mô hình máy chủ tên miền đệm (DNS Caching)



Hình 74: Mô hình máy chủ tên miền đệm

- Các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động, ...) trong mạng của các đơn vị (cơ quan, tổ chức) trước khi kết nối sử dụng dịch vụ (nội bộ hoặc trên Internet) thì việc đầu tiên là phải kết nối, truy vấn tên miền để tìm kiếm thông tin địa chỉ IP của dịch vụ cần kết nối đến.
- Hệ thống DNS Caching sẽ đi tìm kiếm và trả lời các thông tin về tên miền cho các thiết bị trong mạng của các đơn vị đang yêu cầu như hình vẽ trên.

Với các yêu cầu cụ thể:

- Máy chủ DNS: tối thiểu 02 máy chủ DNS Caching với địa chỉ IP khác nhau đặt tại trung tâm TTDL của cơ quan, tổ chức. 02 máy chủ hoạt động Active-Active, đảm bảo khả năng dự phòng nóng, khi 01 máy chủ bị lỗi hoặc hỏng hóc vẫn còn 01 máy chủ còn lại hoạt động, đảm bảo không bị gián đoạn.
- Hệ thống có thể được thiết lập theo cơ chế đệ quy (recursive), tức là sẽ đi tìm kiếm câu trả lời từ các máy chủ DNS khác để trả lời cho máy trạm (client). Hoặc hệ thống có thể được thiết lập theo cơ chế caching forwarder (chuyển tiếp) để chuyển tiếp toàn bộ kết nối, truy vấn tên miền đến hệ thống DNS Caching khác.
- Hệ thống chỉ phục vụ các truy vấn tên miền từ các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động, ...) trong mạng của các đơn vị, không tiếp nhận phục vụ các truy vấn tên miền từ bên ngoài.
- Toàn bộ các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị động, ...) trong mạng của đơn vị phải được cấu hình để sử dụng hệ thống DNS Caching này.
- Ghi nhật ký hoạt động, phần mềm giám sát DNS, phân tích log DNS.
- Triển khai DNSSEC, đóng vai trò xác thực (validation) để đảm bảo an toàn tên miền: DNS Caching hỗ trợ DNSSEC có vai trò rất quan trọng, giúp bảo vệ người sử dụng, chống lại việc giả mạo các phản hồi truy vấn tên miền thông quan việc xác thực chữ ký số trên các bản ghi DNS có trong câu trả lời truy vấn tên miền.
- Triển khai máy chủ DNS chạy song song IPv4, IPv6 (dual-stack), hỗ trợ kết nối, truy vấn từ các máy trạm trên mạng Internet IPv6.
- Thiết lập chính sách tường lửa (firewall): UDP-53, TCP-53 (truy vấn DNS); cho phép truy vấn EDNS(0) (truy vấn DNS hỗ trợ IPv6, DNSSEC).
- Các phần mềm tham khảo: BIND 9.x, Unbound.

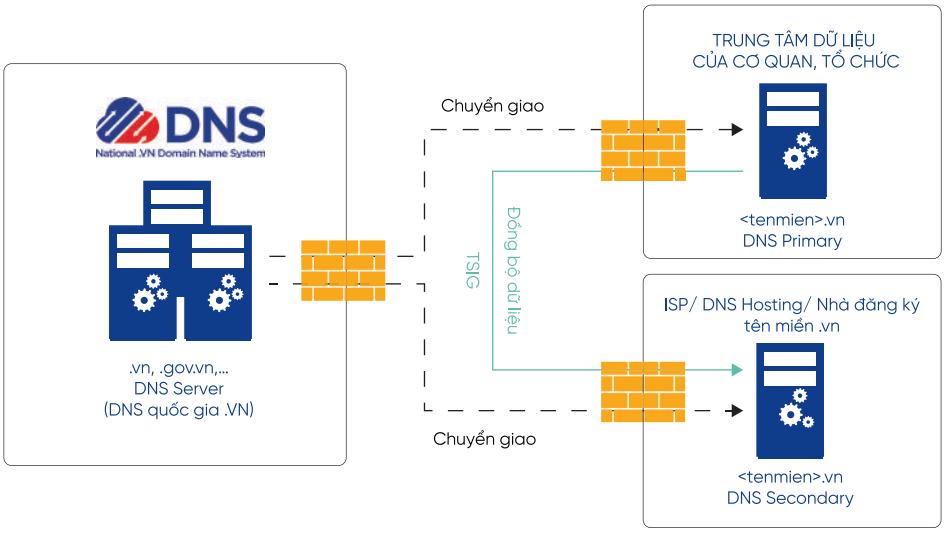
2. Các bài thực hành

2.1. LAB-1: Thiết lập, cài đặt, cấu hình hệ thống Authoritative DNS Server

Bài thực hành thực hiện triển khai hệ thống Authoritative DNS Server quản lý các tên miền của một cơ quan, tổ chức. Hệ thống xây dựng nhằm đáp ứng các yêu cầu và mục tiêu như sau:

- Cài đặt cấu hình các máy chủ DNS hoạt động theo mô hình Master-Slave sử dụng phần mềm BIND.
- Đồng bộ dữ liệu zone sử dụng TSIG nhằm đảm bảo ATTT.
- Nhận truy vấn và phản hồi truy vấn DNS.

Mô hình LAB như sau:



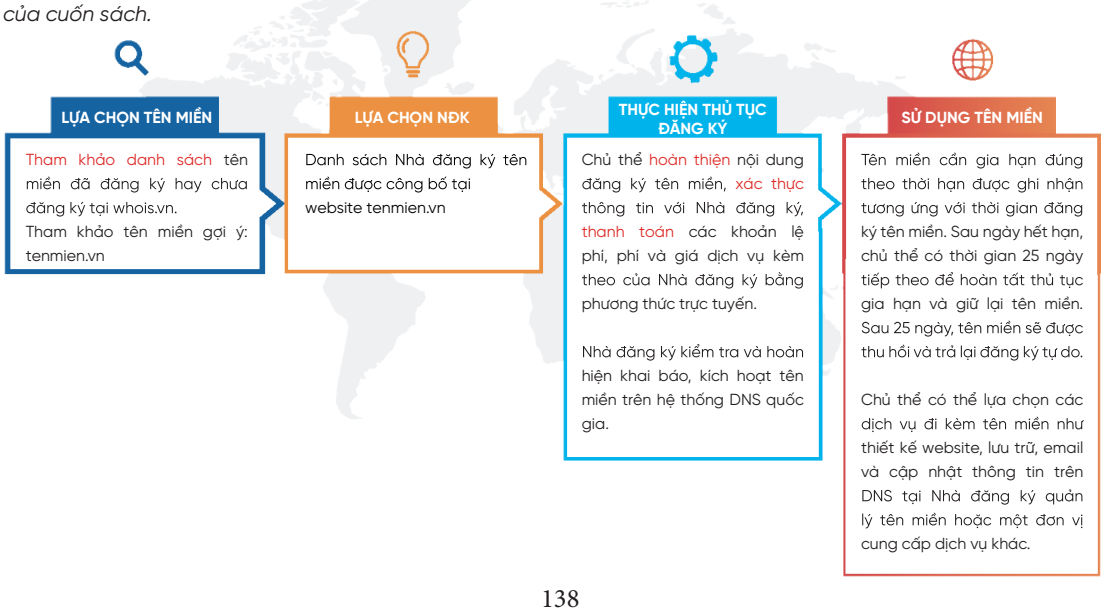
Hình 75: Mô hình Lab-1 – Authortitative DNS Server

LAB-1 sẽ tiến hành thực hiện theo các bài phần sau đây:

- Phần 1 - Cài đặt phần mềm BIND
- Phần 2- Cấu hình BIND
- Phần 3- Khởi tạo dữ liệu zone tên miền
- Phần 4 - Đồng bộ dữ liệu zone tên miền
- Phần 5 - Cập nhật dữ liệu zone tên miền
- Phần 6 - Cấu hình TSIG
- Phần 7 - Cấu hình RNDC
- Phần 8 - Khai báo chuyển giao DNS

Lưu ý: Trước khi đi vào từng phần cài đặt, cấu hình chi tiết. Chúng ta cần tiến hành đăng ký và khai báo sử dụng tên miền .vn

Chi tiết các bước đăng ký, sử dụng tên miền .vn đã được giới thiệu trong Mục III. "Quản lý, đăng ký tên miền" của cuốn sách.



2.1.1. Phần 1: Cài đặt phần mềm BIND

Các bước thực hiện trên máy chủ DNS Primary
Bước 1: Cài đặt phần mềm BIND sử dụng yum (CentOS)
Vào đường dẫn vừa giải nén xong và tiến hành cài đặt

```
# yum install bind
```

Bước 2: Kiểm tra kết quả sau khi cài đặt
Kiểm tra phiên bản đã được cài đặt

```
#  named -V
```

2.1.2. Phần 2: Cấu hình BIND

Bước 1: Khởi tạo file cấu hình và khai báo

```
#  touch /etc/named.conf
```

Sử dụng lệnh "vi" để chỉnh sửa và khai báo các thông tin cấu hình:

```
#  vi /etc/named.conf
```

Sử dụng lệnh "vi" để chỉnh sửa và khai báo các thông tin cấu hình:

```
#  vi /etc/named.conf
```

Nội dung khai báo các thông tin, chính sách chung như sau:

```
options {
directory       "/data/named"; thư mục chứa các file dữ liệu
pid-file        "/var/run-named/named.pid"; file chứa process id của named
version         "not currently available"; không hiển thị version của BIND
            listen-on     {127.0.0.1; <IPv4_DNS_Master>; };
            listen-on-v6          {::1; <IPv6_DNS_Master>; };
            recursion     no;
allow-transfer  {none;};
            allow-query           {
                  127.0.0.1;
                  <IPv4_DNS_Master>;
                  <IPv6_DNS_Master>;
                  <IPv4_DNS_Slave>;
                  <IPv6_DNS_Slave>;
                };
};
```

Nội dung khai báo các thông tin, chính sách chung như sau:

```
logging {
//Log truy van
	channel log_query {
		file "/data/logdns/log_query" versions 5 size 500m;
		severity info;
		print-category yes;
		print-severity yes;
		print-time yes;
		};
	channel log_query1 {
		syslog daemon;
		severity info;
		print-category yes;
		print-severity yes;
		print-time yes;
		};
//Log update
	channel log_update {
		file "/data/logdns/log_update" versions 3 size 50m;
		severity info;
		print-category yes;
		print-severity yes;
		print-time yes;
		};

//Log Zone transfer nhan duoc tu cac may chu khac
	channel "xfer-in_log" {
		file "/data/logdns/log_xfer-in" versions 3 size 50m;
		print-category yes;
		print-severity yes;
		print-time yes;
		} ;

//Log Zone transfer gui den cac may chu khac
	channel "xfer-out_log" {
		file "/data/logdns/log_xfer-out" versions 3 size 50m;
		print-category yes;
		print-severity yes;
		print-time yes;
		} ;
// Log debug
	channel "debug" {
		file "/data/logdns/log_debug" versions 3 size 100m;
		print-time yes;
		print-category yes;
		print-severity yes;
		};
	category "queries" { "log_query"; "log_query1"; };
	category "update" {"log_update";};
	category "xfer-in" { "xfer-in_log"; };
	category "xfer-out" { "xfer-out_log"; };
	category "default" { "debug"; };
	category "security" { "debug"; };
	category "config" { "debug"; };
	category "notify" { "debug"; };
	category "lame-servers" { "debug"; };

    };
```

Bước 2: Khai báo thông tin zone tên miền
Khai báo zone Root hints:

```
zone "." in {
        type hint;
        file "named.root";
```

Khai báo zone tên miền quản lý (thay thông tin zone tên miền quản lý **<ten_mien>.vn** bằng tên miền đã được đăng ký trước khi thực hiện các bước cài đặt máy chủ DNS)

```
//khai bao zone ten mien quan ly: <ten_mien>.vn
zone "<ten_mien>.vn" in {
        type master;
        file "db.<ten_mien>.vn";
        };
```

Khai báo các zone local:

```
//khai bao zone localhost (loopback)
zone "localhost" in {
        type master;
        file "db.localhost";
};
//khai bao zone ten mien nguoc localhost (loopback IPv4)
zone "0.0.127.in-addr.arpa" in {
        type master;
        file "db.ipv4-rev-loopback";
};
//khai bao zone ten mien nguoc localhost (loopback IPv6)
zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" {
      type master;
      file "db.ipv6-rev-loopback";
};
```

Bước 3: Kiểm tra thông tin file cấu hình
Sử dụng lệnh named-checkconf:

```
#  named-checkconf /etc/named.conf
```

2.1.3. Phần: Khởi tạo dữ liệu:

Bước 1: Khởi tạo dữ liệu zone tên miền
Khởi tạo các dữ liệu zone tên miền: Với mỗi zone được khai báo trong file cấu hình sẽ khởi tạo tương ứng từng file dữ liệu zone tên miền.
Khởi tại file dữ liệu zone tên miền quản lý:

```
#  vi /data/named/db.<ten_mien>.vn

//khai bao du lieu zone ten mien quan ly
$TTL    43200
@       IN    SOA   dns-master.<ten_mien>.vn.      postmaster.<ten_mien>.vn. (
                        2020050501    ; serial
                        3600          ; refresh (1 hour)
                        1800          ; retry (30 minutes)
                        604800         ; expire (1 week)
                        5400          ; minimum (1 hour 30 minutes)
                        )
NS      ns1.<ten_mien>.vn.
NS      ns2.<ten_mien>.vn.
MX    10      mail1.<ten_mien>.vn.
```

```
MX    20      mail2.<ten_mien>.vn.

$ORIGIN <ten_mien>.vn.
www   IN      A           192.168.2.17
          IN      AAAA       2001:de8:a:2::17
mail      IN      A            192.168.2.20
          IN      AAAA       2001:de8:a:2::20
mail1    IN      A            192.168.2.18
mail2    IN      A            192.168.2.19
```

Khởi tạo các file dữ liệu zone local:

```
#  vi /data/named/db.localhost
```

```
//khai bao du lieu zone localhost (loopback)
$TTL    43200
@       IN      SOA   localhost.        root.localhost. (
                      1                  ; serial
                      3600               ; refresh (1 hour)
                      1800               ; retry (30 minutes)
                      604800             ; expire (1 week)
                      5400               ; minimum (1 hour 30 minutes)
                      )
        NS      localhost.
        A       127.0.0.1
        AAAA    ::1
```

Khởi tạo các file dữ liệu zone tên miền ngược local:

```
#  vi /data/named/db.ipv4-rev-loopback
```

```
//khai bao du lieu zone ten mien nguoc localhost (loopback ipv4)
$TTL    43200
@       IN      SOA   localhost.        root.localhost. (
                      1                  ; serial
                      3600               ; refresh (1 hour)
                      1800               ; retry (30 minutes)
                      604800             ; expire (1 week)
                      5400               ; minimum (1 hour 30 minutes)
                      )
        NS      localhost.
        PTR     localhost.
```

```
#  vi /data/named/db.ipv6-rev-loopback
```

```
//khai bao du lieu zone ten mien nguoc localhost (loopback ipv6)
$TTL    43200
@       IN      SOA   localhost.        root.localhost. (
                      1                  ; serial
                      3600               ; refresh (1 hour)
                      1800               ; retry (30 minutes)
                      604800             ; expire (1 week)
                      5400               ; minimum (1 hour 30 minutes)
                      )
        NS      localhost.
        PTR     localhost.
```

Khởi tạo dữ liệu zone Root hints (Thông tin chính thức trên website IANA: https://www.iana.org/domains/root/files)

```
# vi /data/named/named.root

;       This file holds the information on root DNS Servers needed to
;       initialize cache of Internet domain DNS Servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain DNS Servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     April 10, 2025
;       related version of root zone:     2025041001
;
; FORMERLY NS.INTERNIC.NET
;
.                       3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     170.247.170.2
B.ROOT-SERVERS.NET.     3600000      AAAA  2801:1b8:10::b
;
...
```

Bước 2: Kiểm tra thông tin file dữ liệu zone tên miền
Kiểm tra thông tin các file dữ liệu zone tên miền sử dụng các lệnh named-checkzone như sau:

```
# named-checkzone <ten_mien>.vn /data/named/db.<ten_mien>.vn
# named-checkzone <zone> /data/named/<zone_file>
```

Bước 3: Khởi động dịch vụ DNS (named)

```
# systemctl start named
```

Kiểm tra tiến trình named:

```
# ps aux | grep named
```

Bước 4: Kiểm tra hoạt động DNS
Sử dụng câu lệnh "dig" hoặc "nslookup" để kiểm tra hoạt động DNS sau khi cấu hình:
Truy vấn DNS theo thông tin tên miền đã khai báo

```
# nslookup
> server <IPv4/IPv6_DNS_Master>
> set type=A
> www.<ten_mien>.vn
```

```
# dig @<IPv4/IPv6_DNS_Master> <ten_mien> <loai_ban_ghi> [+option]
VD:
# dig @192.168.1.12 www.vnnic.vn A +norec
```

2.1.4. Phần 4: Đồng bộ dữ liệu zone tên miền

Bước 1: Cấu hình đồng bộ zone tên miền trên máy chủ DNS Primary
Sử dụng lệnh "vi" để chỉnh sửa và khai báo các thông tin đồng bộ dữ liệu zone tên miền:

```
#  vi /etc/named.conf
```

Chỉnh sửa các thông tin sau trong file cấu hình named.conf:

```
options {
…
allow-transfer  {
                    IPv4_DNS_Slave_01;
                    IPv4_DNS_Slave_02;
                   };
notify              yes;
…
};
```

Kiểm tra thông tin file cấu hình sử dụng lệnh named-checkconf:

```
#  named-checkconf /etc/named.conf
```

Bước 2: Cấu hình đồng bộ zone tên miền trên các máy chủ DNS Secondary
Sử dụng lệnh "vi" để chỉnh sửa và khai báo các thông tin đồng bộ dữ liệu zone tên miền:

```
#  vi /etc/named.conf
```

Chỉnh sửa các thông tin sau trong file cấu hình named.conf:

```
options {
…
notify              yes;
…
};
```

Khai báo zone tên miền đồng bộ từ DNS Primary:

```
//khai bao zone ten mien dong bo: <ten_mien>.vn
zone "<ten_mien>.vn" in {
      type slave;
      masters { <IPv4_DNS_Master>; };
      file "db.<ten_mien>.vn";
      };
```

Kiểm tra thông tin file cấu hình sử dụng lệnh named-checkconf:

```
#  named-checkconf /etc/named.conf
```

Bước 3: Khởi động lại dịch vụ DNS (named)
Kiểm tra và tạm dừng tiến trình named đang chạy:

```
#  systemctl status named
```

Khởi động lại dịch vụ named:

```
# systemctl restart named
```

Kiểm tra tiến trình named:

```
# systemctl status named
```

Bước 4: Kiểm tra hoạt động đồng bộ dữ liệu zone tên miền
Kiểm tra trong log transfer:
Trên máy chủ DNS Master:

```
# vi /etc/named.conf
```

Trên các máy chủ DNS Slave:

```
# more /data/logdns/log_xfer-in
```

Kiểm tra thông tin truy vấn tên miền trên các máy chủ DNS Slave:

```
# nslookup
> server <IPv4/IPv6_DNS_Slave>
> set type=A
> www.<ten_mien>.vn
```

```
# dig @<IPv4/IPv6_DNS_Slave> <ten_mien> <loai_ban_ghi> [+option]
VD:
# dig @192.168.1.12 www.vnnic.vn A +norec
```

2.1.5. Phần 5: Cập nhật dữ liệu zone tên miền

Trong phần này các nhóm sẽ tiến hành thực hiện cập dữ liệu zone tên miền bằng phương pháp thủ công (Manual) và cập nhật động Dynamic Update (NSUPDATE) trên máy chủ DNS Primay:

(1) Phương pháp 1: Cập nhật thủ công (Manual)

Bước 1: Khai báo thông tin tên miền cần cập nhật vào zone tên miền
Sử dụng lệnh "vi" để chỉnh sửa cập nhật thông tin tên miền trong zone cần cập nhật

```
# vi /data/named/db.<ten_mien>.vn
```

```
$TTL    43200
@       IN    SOA   dns-master.<ten_mien>.vn.      postmaster.<ten_mien>.vn. (
                        2020050501     ; serial
                        3600           ; refresh (1 hour)
                        1800           ; retry (30 minutes)
                        604800          ; expire (1 week)
                        5400           ; minimum (1 hour 30 minutes)
                        )
NS      ns1.<ten_mien>.vn.
NS      ns2.<ten_mien>.vn.
MX    10      mail1.<ten_mien>.vn.
MX    20      mail2.<ten_mien>.vn.

$ORIGIN <ten_mien>.vn.
www   IN      A           192.168.2.17
          IN      AAAA      2001:de8:a:2::17
mail      IN      A          192.168.2.20
          IN      AAAA      2001:de8:a:2::20
mail1     IN      A          192.168.2.18
mail2     IN      A          192.168.2.19
dvc       IN      A          10.10.0.20
          IN      AAAA      2001:dc8:1000::23
```

Bước 2: Tăng giá trị Serial Number

```
$TTL    43200
@       IN      SOA     dns-master.<ten_mien>.vn.       postmaster.<ten_mien>.vn. (
                        2020050502      ; serial
                        3600            ; refresh (1 hour)
                        1800            ; retry (30 minutes)
                        604800          ; expire (1 week)
                        5400            ; minimum (1 hour 30 minutes)
                        )
NS      ns1.<ten_mien>.vn.
NS      ns2.<ten_mien>.vn.
MX    10      mail1.<ten_mien>.vn.
MX    20      mail2.<ten_mien>.vn.

$ORIGIN <ten_mien>.vn.
www   IN      A           192.168.2.17
          IN      AAAA      2001:de8:a:2::17
mail      IN      A          192.168.2.20
          IN      AAAA      2001:de8:a:2::20
mail1     IN      A          192.168.2.18
mail2     IN      A          192.168.2.19
dvc       IN      A          10.10.0.20
          IN      AAAA      2001:dc8:1000::23
```

Bước 3: Khởi động lại named
Kiểm tra file dữ liệu zone vừa chỉnh sửa

```
#  named-checkzone <ten_mien>.vn /data/named/db.<ten_mien>.vn
#  named-checkzone <zone> /data/named/<zone_file>
```

Kiểm tra và tạm dừng tiến trình named đang chạy:

```
#  systemctl status named
```

Khởi động lại dịch vụ named:

```
#  systemctl restart named
```

Kiểm tra tiến trình named:

```
#  systemctl status named
```

Bước 4: Kiểm tra truy vấn thông tin tên miền sau khi cập nhật

```
#  nslookup
>  server <IPv4/IPv6_DNS_Slave>
>  set type=A
>  dvc.<ten_mien>.vn
```

```
#  dig @<IPv4/IPv6_DNS_Slave> <ten_mien> <loai_ban_ghi> [+option]
VD:
#  dig @192.168.1.12 dvc.vnnic.vn A +norec
```

(2) Phương pháp 2: Dynamic Update (NSUPDATE)

Bước 1: Chỉnh sửa cấu hình named.conf trên DNS Master cho phép update bằng phương pháp Dynamic Update:

```
options {
...
allow-update {<IPv4/IPv6_DNS_Master>;};
...
};
```

Bước 2: Khởi động lại named để nhận cấu hình mới
Kiểm tra và tạm dừng tiến trình named đang chạy:

```
# systemctl status named
```

Khởi động lại dịch vụ named:

```
# systemctl restart named
```

Kiểm tra tiến trình named:

```
# systemctl status named
```

Bước 4: Kiểm tra truy vấn thông tin tên miền sau khi cập nhật

```
# nslookup
> server <IPv4/IPv6_DNS_Slave>
> set type=A
> dichvucong.<ten_mien>.vn
```

```
# dig @<IPv4/IPv6_DNS_Slave> <ten_mien> <loai_ban_ghi> [+option]
VD:
# dig @192.168.1.12 dichvucong.vnnic.vn A +norec
```

2.1.6. Phần 6: TSIG

Bước 1: Tạo khóa chung TSIG trên DNS Primary

```
# dnssec-keygen -r /dev/urandom -a HMAC-MD5 -b 128 -n HOST tsig-
```

Kết quả:

```
# Ktsig-key.+157+33570
```

Sau khi thực hiện lệnh tạo khóa, sẽ tạo ra một cặp khóa Public-Private Key:

```
-rw-------. 1 root root    52 May 18 00:02 Ktsig-key.+157+33570.key
-rw-------. 1 root root   165 May 18 00:02 Ktsig-key.+157+33570.private
```

Bước 2: Khai báo TSIG trên DNS Primary
Đọc thông tin khóa vừa tạo

```
# cat Ktsig-key.+157+33570.private
```

Thông tin khóa có dạng:

```
Private-key-format: v1.3
Algorithm: 157 (HMAC_MD5)
Key: r3yyrn4DANX+tAvntlrbig==
Bits: AAA=
```

Tạo file cấu hình TSIG trên DNS Primary

```
# vi /etc/tsig.key
```

Tạo file cấu hình TSIG trên DNS Primary

```
key "TRANSFER" {
        algorithm hmac-md5;
        secret " r3yyrn4DANX+tAvntlrbig==";
};
# Slave server IP # 1
server <IP_DNS_Slave> {
       keys {
            TRANSFER;
   };
};
```

Chèn đường dẫn đến file cấu hình thông tin TSIG trong named.conf

```
include "/etc/tsig.key";
```

Khởi động lại dịch vụ named trên DNS Primary:
Kiểm tra và tạm dừng tiến trình named đang chạy:

```
#  systemctl status named
```

Khởi động lại dịch vụ named:

```
#  systemctl restart named
```

Kiểm tra tiến trình named:

```
#  systemctl status named
```

Bước 3: Cấu hình TSIG trên DNS Secondary:
Tạo file cấu hình thông tin TSIG như trên DNS Primary:

```
# vi /etc/tsig.key
```

Với nội dung như sau:

```
key "TRANSFER" {
        algorithm hmac-md5;
        secret " r3yyrn4DANX+tAvntlrbig==";
};
# Master Server IP
server <IP_DNS_Master> {
       keys {
            TRANSFER;
   };
};
```

Chèn đường dẫn đến file cấu hình thông tin TSIG trong named.conf

```
include "/etc/tsig.key";
```

Khởi động lại dịch vụ named trên DNS Secondary:
Kiểm tra và tạm dừng tiến trình named đang chạy:

```
# systemctl status named
```

Khởi động lại dịch vụ named:

```
# systemctl restart named
```

Kiểm tra tiến trình named:

```
# systemctl status named
```

Bước 4: Cấu hình đồng bộ zone transfer sử dụng TSIG:
Chỉnh sửa thông tin file cấu hình named.conf trên DNS Primary như sau:

```
# vi /etc/named.conf
```

Với các nội dung như sau:

```
options {
...
allow-transfer {  key TRANSFER; };
...
};
```

Khởi động lại dịch vụ named trên DNS Primary:
Kiểm tra và tạm dừng tiến trình named đang chạy:

```
# systemctl status named
```

Khởi động lại dịch vụ named:

```
# systemctl restart named
```

Kiểm tra tiến trình named:

```
# systemctl status named
```

2.1.7. Phần 7: RNDC

Bước 1: Thực thi lệnh tạo chuỗi khóa của RNDC

```
# rndc-confgen
```

Kết quả sau khi thực thi lệnh như sau:

```
# Start of rndc.conf
key “rndc-key” {
        algorithm hmac-md5;
        secret “qIq+lcGp2xSkrm7vXIvEbA==”;
};

options {
        default-key “rndc-key”;
        default-server 127.0.0.1;
        default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as needed:
# key “rndc-key” {
#       algorithm hmac-md5;
#       secret “qIq+lcGp2xSkrm7vXIvEbA==”;
# };
#
# controls {
#       inet 127.0.0.1 port 953
#               allow { 127.0.0.1; } keys { “rndc-key”; };
# };
# End of named.conf
```

Bước 2: Khởi tạo và cấu hình file rndc.conf

Sử dụng lệnh “vi” để khởi tạo file rndc.conf và sao chép phần nội dung của kết quả vừa tạo ra: bắt đầu từ “#

```
# vi /etc/rndc.conf
```

```
# Start of rndc.conf
key “rndc-key” {
        algorithm hmac-md5;
        secret “qIq+lcGp2xSkrm7vXIvEbA==”;
};

options {
        default-key “rndc-key”;
        default-server 127.0.0.1;
        default-port 953;
};
```

Bước 3: Khai báo thông tin chuỗi khóa rndc trong named.conf:

Mở và chỉnh sửa file cấu hình named.conf, sao chép phần nội dung còn lại của kết quả sau khi thực thi lệnh rndc-confgen vào trong phần khai báo của file named.conf:

```
# vi /etc/named.conf
```

```
# Use with the following in named.conf, adjusting the allow list as needed:
key “rndc-key” {
        algorithm hmac-md5;
        secret “qIq+lcGp2xSkrm7vXIvEbA==”;
};
 controls {
        inet 127.0.0.1 port 953
        allow { 127.0.0.1; } keys { “rndc-key”; };
};
# End of named.conf
```

Bước 4: Khởi động lại dịch vụ named

Kiểm tra và tạm dừng tiến trình named đang chạy:

```
#  systemctl status named
```

Khởi động lại dịch vụ named:

```
#  systemctl restart named
```

Kiểm tra tiến trình named:

```
#  systemctl status named
```

Bước 5: Kiểm tra hoạt động RNDC

```
# rndc status
version: BIND 9.14.2 <id:2c2bc60> (wow ...)
running on dns-cache-01.vnnic.vn: Linux x86_64 2.6.32-431.el6.x86_64 #1 SMP Sun Nov 10 22:19:54
EST 2013
boot time: Mon, 30 Sep 2019 09:05:35 GMT
last configured: Mon, 30 Sep 2019 09:05:35 GMT
configuration file: /etc/named.conf
CPUs found: 2
worker threads: 2
UDP listeners per interface: 1
number of zones: 101 (98 automatic)
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is ON
recursive clients: 0/900/1000
tcp clients: 0/150
server is up and running
```

Lưu ý:

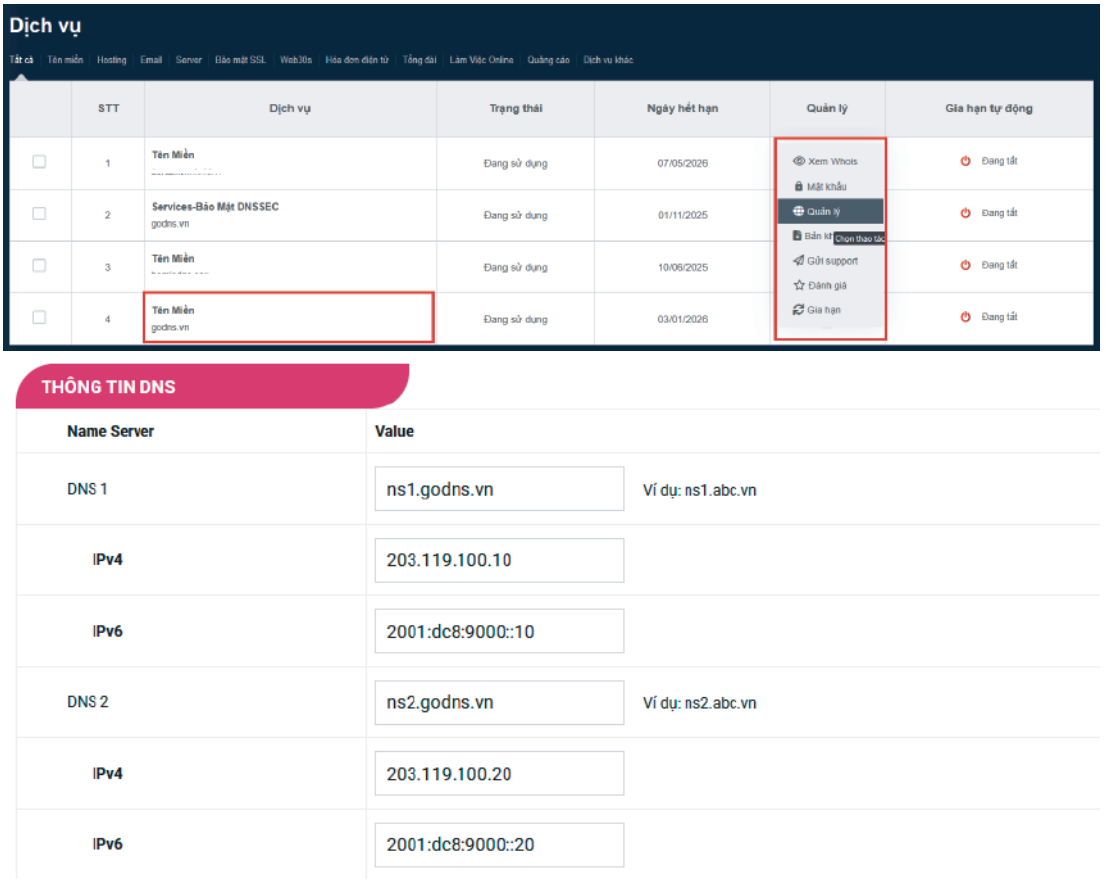
Sau khi cài đặt, cấu hình và tối ưu các máy chủ DNS cần đảm bảo rằng các máy chủ DNS đã được thiết lập chính sách mở cổng 53/UDP và cổng 53/TCP (đây là cổng, giao thức được sử dụng cho dịch vụ DNS)

2.1.8. Phần 8: Khai báo chuyển giao DNS và các dịch vụ

Sau khi hoàn tất các bước cài đặt máy chủ DNS, để đảm bảo hệ thống có thể hoạt động trên Internet, chúng ta cần tiến hành khai báo chuyển giao tên miền (đã được đăng ký trong phần đầu tiên) trên hệ thống máy chủ tên miền (DNS) quốc gia ".vn" về các máy chủ DNS vừa được thiết lập thông qua hệ thống quản lý (Portal) của Nhà đăng ký tên miền. (Thông thường các tên miền vừa được đăng ký thành công, tên miền sẽ được khai báo máy chủ DNS chuyển giao mặc định là các máy chủ DNS của chính Nhà đăng ký đó).

Bước 1: Tiến hành thực hiện khai báo chuyển giao về máy chủ DNS vừa thiết lập.
Ví dụ minh họa dưới đây cho tên miền godns.vn (thông tin địa chỉ IP đã được thay đổi):

MÁY CHỦ CHUYỂN GIAO		
Hostname	Địa chỉ IPv4	Địa chỉ IPv6
ns1.godns.vn	203.119.100.10	2001:dc8:9000::10
ns2.godns.vn	203.119.100.20	2001:dc8:9000::20



Hình 76: Ví dụ minh họa cập nhật bản ghi NS

(*) Thông thường sau khi cập nhật khai báo máy chủ DNS chuyển giao sẽ mất khoảng 5 phút để đồng bộ lên hệ thống máy chủ tên miền (DNS) quốc gia ".vn".

(**) Khai báo tối thiểu 02 máy chủ DNS chuyển giao.

Bước 2: Sử dụng công cụ WHOIS của VNNIC (http://whois.vnnic.vn) để kiểm tra thông tin vừa được cập nhật, khai báo chuyển giao DNS trên hệ thống máy chủ tên miền (DNS) quốc gia.

Hình 77: Ví dụ minh họa tra cứu WHOIS

(*) Kết quả tra cứu WHOIS như sau:

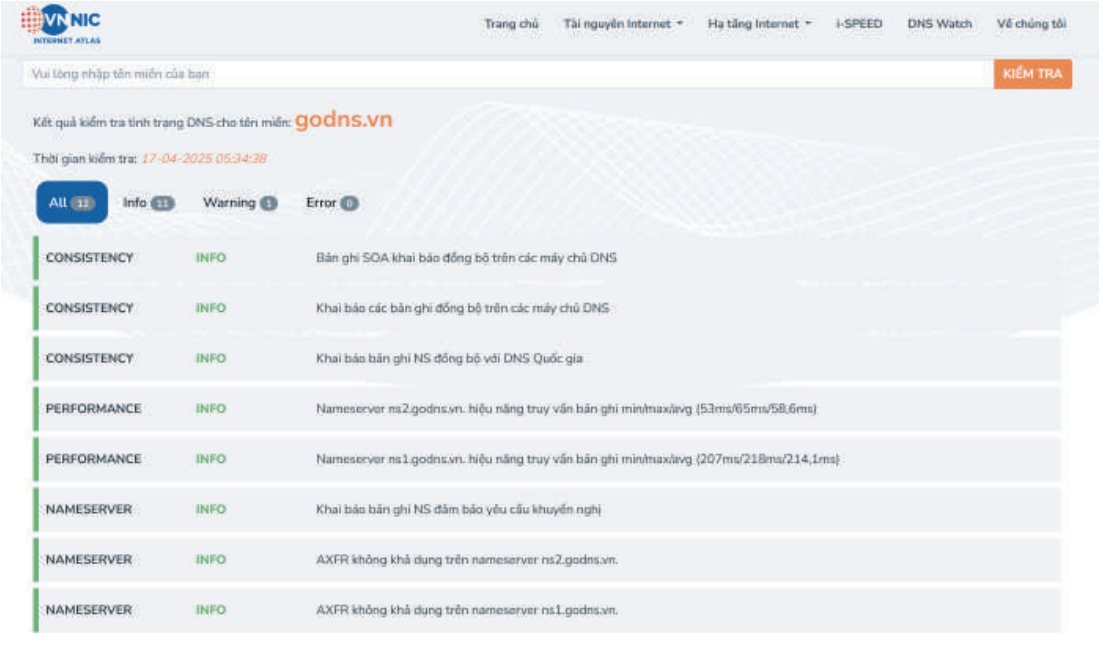
Kết quả tra cứu thông tin tên miền

Tên miền:	godns.vn
Tên chủ thể đăng ký sử dụng:	
Nhà đăng ký quản lý:	Công ty TNHH P.A Việt Nam
Ngày đăng ký:	2024-01-03
Ngày hết hạn:	2026-01-03
Trạng thái:	clientTransferProhibited
Máy chủ DNS chuyển giao:	ns1.godns.vn ns2.godns.vn
DNSSEC:	Chưa ký

Hình 78: Ví dụ minh họa kết quả tra cứu WHOIS

Bước 3: Kiểm tra, tối ưu các thông tin bằng các công cụ kiểm tra sức khỏe hệ thống.

- Sử dụng công cụ DNS Watch của VNNIC (https://internetatlas.vnnic.vn/dns-watch)



Hình 79: Kiểm tra tên miền bằng công cụ DNS Watch by VNNIC

- Sử dụng công cụ dig hoặc nslookup

```
~$ dig @b.dns-servers.vn godns.vn NS +norec
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @b.dns-servers.vn godns.vn NS +norec
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64294
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 06c633ae4b189fa4f161ff9568003161340c1cf647f1d4f5 (good)
;; QUESTION SECTION:
;godns.vn.                IN     NS

;; AUTHORITY SECTION:
godns.vn.          43200  IN     NS     ns2.godns.vn.
godns.vn.          43200  IN     NS     ns1.godns.vn.

;; Query time: 30 msec
;; SERVER: 203.119.73.105#53(b.dns-servers.vn) (UDP)
;; WHEN: Wed Apr 16 22:38:25 UTC 2025
;; MSG SIZE  rcvd: 118
```

Bước 4: Khai báo các bản ghi sử dụng cho các dịch vụ trên Internet tương ứng với tên miền.

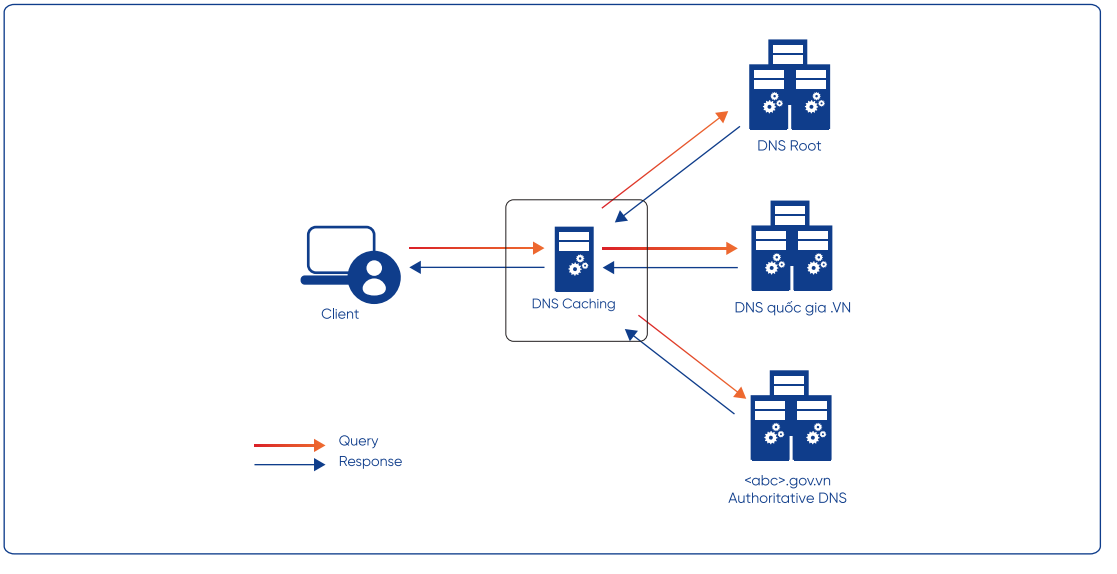
LOẠI BẢN GHI	DỊCH VỤ	VÍ DỤ
A/AAAA	Website	www.godns.vn IN A 202.113.10.201 www.godns.vn IN AAAA 2001:dc8::2
MX	Mail exchange	godns.vn IN MX 10 mail1.godns.vn. godns.vn IN MX 10 mail2.godns.vn.
TXT	Xác thực email (SPF/ DKIM/ DMARC)	godns.vn IN TXT "v=spf1 a mx" _dmarc.godns.vn IN TXT "v=DMARC1; p=reject"

2.2. LAB-2: Thiết lập, cài đặt, cấu hình hệ thống DNS Caching

Bài thực hành thực hiện triển khai hệ thống DNS Caching cho cơ quan, đơn vị. Hệ thống xây dựng nhằm đáp ứng các yêu cầu và mục tiêu như sau:

- Cài đặt cấu hình các máy chủ DNS hoạt động đúng chức năng DNS Caching (DNS Resolver – máy chủ phân giải đệ quy) sử dụng phần mềm BIND.
- Cấu hình chuyển tiếp truy vấn tên miền .VN
- Nhận truy vấn và phản hồi truy vấn DNS

Mô hình LAB như sau:



Hình 80: Mô hình Lab-2 - DNS Caching

Bài thực hành 2 sẽ tiến hành thực hiện theo các bài phần sau đây:

- Phần 1 - Cài đặt phần mềm BIND
- Phần 2- Cấu hình BIND (DNS Caching)
- Phần 3- Kiểm tra hoạt động truy vấn và phản hồi truy vấn DNS
- Phần 4- Kết nối và sử dụng

2.2.1. Phần 1: Cài đặt, cấu hình phần mềm BIND

Bước 1: Thực hiện cài đặt bằng yum (CentOS)

```
# yum install bind
```

Bước 2: TKiểm tra kết quả sau khi cài đặt
Kiểm tra phiên bản đã được cài đặt

```
# named -V
```

2.2.2. Phần 2: Cấu hình BIND (DNS Caching)

Bước 1: Khởi tạo file cấu hình và khai báo

```
# touch /etc/named.conf
```

Nội dung khai báo các thông tin, chính sách chung như sau:

```
options {
directory       "/data/named"; thu muc chua cac file du lieu
pid-file        "/var/run-named/named.pid"; file chua process id của named
version         "not currently available"; khong hien thi verion cua bind
                listen-on     {127.0.0.1; <IPv4_DNS_Caching>; };
//lang nghe tren dia chi loopback va dia chi IPv4 cua DNS Caching
                listen-on-v6            {::1; <IPv6_DNS_Caching>; };
//lang nghe tren dia chi loopback va dia chi IPv6 cua DNS Caching
                recursion    yes; cho phep de quy
                allow-query             {any;};
//cho phep truy van tu bat ky dia chi IP nao
};
```

Khai báo thông tin cấu hình log:

```
logging {
//Log truy van
        channel log_query {
                file "/data/logdns/log_query" versions 5 size 500m;
                severity info;
                print-category yes;
                print-severity yes;
                print-time yes;
                };
        channel log_query1 {
                syslog daemon;
                severity info;
                print-category yes;
                print-severity yes;
                print-time yes;
                };
// Log debug
        channel "debug" {
                file "/data/logdns/log_debug" versions 3 size 100m;
```

```
            print-time yes;
            print-category yes;
            print-severity yes;
            };
        category "queries" { "log_query"; "log_query1"; };
        category "default" { "debug"; };
        category "security" { "debug"; };
        category "config" { "debug"; };
        category "notify" { "debug"; };
        category "lame-servers" { "debug"; };

      };
```

Khai báo zone Root hints:

```
zone "." in {
      type hint;
      file "named.root";
      };
```

Bước 2: Kiểm tra thông tin file cấu hình
Sử dụng lệnh named-checkconf:

```
#  named-checkconf /etc/named.conf
```

Bước 3: Khởi tạo dữ liệu zone tên miền
Khởi tạo dữ liệu zone Root hints (Thông tin chính thức trên website IANA: https://www.iana.org/domains/root/files)

```
#  vi /data/named/named.root
```

```
;      This file holds the information on root DNS Servers needed to
;      initialize cache of Internet domain DNS Servers
;      (e.g. reference this file in the "cache  .  <file>"
;      configuration file of BIND domain DNS Servers).
;
;      This file is made available by InterNIC
;      under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;      -OR-                     RS.INTERNIC.NET
;
;      last update:     April 10, 2025
;      related version of root zone:     2025041001
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     170.247.170.2
B.ROOT-SERVERS.NET.      3600000      AAAA  2801:1b8:10::b
;
...
```

2.2.3. Phần 3: Kiểm tra hoạt động truy vấn và phản hồi truy vấn DNS

Lưu ý:

Sau khi cài đặt, cấu hình và tối ưu các máy chủ DNS cần đảm bảo rằng các máy chủ DNS đã được thiết lập chính sách mở cổng 53/UDP và cổng 53/TCP (đây là cổng, giao thức được sử dụng cho dịch vụ DNS)

Bước 1: Sử dụng các công cụ để kiểm tra hoạt động truy vấn/ phản hồi truy vấn DNS

```
# dig @192.168.10.100 youtube.com AAAA
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @192.168.10.100 youtube.com
AAAA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12028
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7f52629d4249328501000000006800368298a2501feb8e13a6 (good)
;; QUESTION SECTION:
;youtube.com.                   IN      AAAA

;; ANSWER SECTION:
youtube.com.            300     IN      AAAA    2404:6800:4005:821::200e

;; Query time: 750 msec
;; SERVER: 192.168.10.100#53(192.168.10.100) (UDP)
;; WHEN: Wed Apr 16 23:00:18 UTC 2025
;; MSG SIZE  rcvd: 96
```

Bước 2: Kiểm tra log hệ thống

Như đã thực hành cấu hình ở trên, phần log hệ thống gồm các log quan trọng như:

(1) Log mặc định của hệ thống

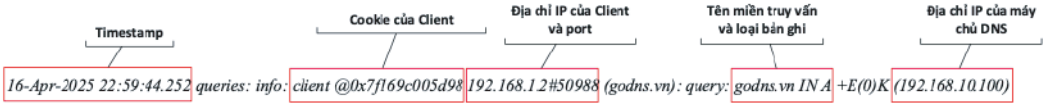
- Đường dẫn mặc định của log hệ thống đối với hệ điều hành Redhat/CentOS sẽ nằm trong (/var/log/messages), còn đối với các hệ điều hành Debian/Ubuntu sẽ nằm trong (/var/log/syslog)

```
2025-04-16T22:58:51.775831+00:00 trinv-pc named[3251]: configuring command channel from '/etc/bind/rndc.key'
2025-04-16T22:58:51.775853+00:00 trinv-pc named[3251]: command channel listening on 127.0.0.1#953
2025-04-16T22:58:51.775893+00:00 trinv-pc named[3251]: configuring command channel from '/etc/bind/rndc.key'
2025-04-16T22:58:51.775936+00:00 trinv-pc named[3251]: command channel listening on ::1#953
2025-04-16T22:59:11.160643+00:00 trinv-pc systemd[1]: Starting named.service - BIND Domain DNS Server...
```

(2) Log truy vấn DNS

```
# tail -f /data/logdns/log_query
16-Apr-2025 22:59:18.602 queries: info: client @0x7f1698003708 192.168.1.2#38897 (vnnic.vn): query: vnnic.vn IN A +E(0)K (192.168.10.100)
16-Apr-2025 22:59:44.252 queries: info: client @0x7f169c005d98 192.168.10.100#50988 (godns.vn): query: godns.vn IN A +E(0)K (192.168.10.100)
16-Apr-2025 22:59:53.092 queries: info: client @0x7f16a42a9678 192.168.1.2#54581 (vnexpres.vn): query: vnexpres.vn IN A +E(0)K (192.168.10.100)
16-Apr-2025 22:59:55.532 queries: info: client @0x7f1694003928 192.168.1.2#57452 (vnexpres.vn): query: vnexpres.vn IN AAAA +E(0)K (192.168.10.100)
16-Apr-2025 22:59:58.662 queries: info: client @0x7f168c003328 192.168.1.2#58094 (vnexpres.vn): query: vnexpres.vn IN MX +E(0)K (192.168.10.100)
16-Apr-2025 23:00:02.882 queries: info: client @0x7f16a42a9678 192.168.1.2#52535 (vnexpress.vn): query: vnexpress.vn IN MX +E(0)K (192.168.10.100)
```

```
16-Apr-2025 23:00:06.622 queries: info: client @0x7f169c005d98 192.168.1.2#33166 (vnexpress.vn): query: vnexpress.vn IN AAAA +E(0)K (192.168.10.100)
16-Apr-2025 23:00:17.312 queries: info: client @0x7f1684003bd8 192.168.1.2#34801 (youtube.com): query: youtube.com IN AAAA +E(0)K (192.168.10.100)
```



Hình 81: Định dạng log phần mềm BIND

(3) Log debug (các thông báo lỗi, trạng thái,...) của DNS

Phần thông tin log debug của hệ thống DNS như đã thiết lập trong phần trên sẽ lại các thông tin chi tiết về quá trình hoạt động của máy chủ DNS, đặc biệt trong các tình huống lỗi hoặc trong quá trình hoạt động và khắc phục sự cố. Cài đặt chế độ debug logging giúp quản trị hệ thống dễ dàng theo dõi các hành động của máy chủ DNS và xác định nguyên nhân của các vấn đề có thể phát sinh trong quá trình phân giải tên miền (như liên quan đến network, dnssec,...).

Chi tiết log debug nên được ghi ra một file riêng (/data/logdns/log_debug)

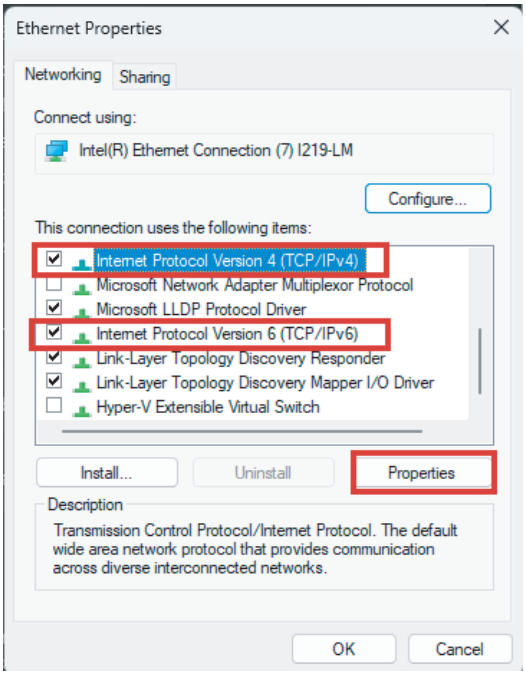
```
16-Apr-2025 22:59:13.332 general: info: received control channel command 'stop'
16-Apr-2025 22:59:13.332 network: info: no longer listening on 127.0.0.1#53
16-Apr-2025 22:59:13.332 network: info: no longer listening on 172.29.29.72#53
16-Apr-2025 22:59:13.332 network: info: no longer listening on ::1#53
16-Apr-2025 22:59:13.342 network: info: no longer listening on fe80::215:5dff:fe12:b9ab%2#53
16-Apr-2025 22:59:13.342 general: info: shutting down: flushing changes
16-Apr-2025 22:59:13.342 general: notice: stopping command channel on 127.0.0.1#953
16-Apr-2025 22:59:13.342 general: notice: stopping command channel on ::1#953
16-Apr-2025 22:59:13.362 general: notice: exiting
16-Apr-2025 22:59:13.412 zoneload: info: managed-keys-zone: loaded serial 4
16-Apr-2025 22:59:13.412 zoneload: info: zone 0.in-addr.arpa/IN: loaded serial 1
16-Apr-2025 22:59:13.422 zoneload: info: zone 127.in-addr.arpa/IN: loaded serial 1
16-Apr-2025 22:59:13.422 zoneload: info: zone localhost/IN: loaded serial 2
16-Apr-2025 22:59:13.422 zoneload: info: zone 255.in-addr.arpa/IN: loaded serial 1
16-Apr-2025 22:59:13.422 general: notice: all zones loaded
16-Apr-2025 22:59:13.422 general: notice: running
```

2.2.4. Phần 4: Kết nối và sử dụng

Sau khi thực hiện bước kiểm tra các hoạt động của hệ thống DNS Caching và không phát hiện bất kỳ lỗi nào, người dùng có thể thực hiện cấu hình khai báo, thay đổi thông tin máy chủ DNS (DNS Servers) trên thiết bị của người dùng:

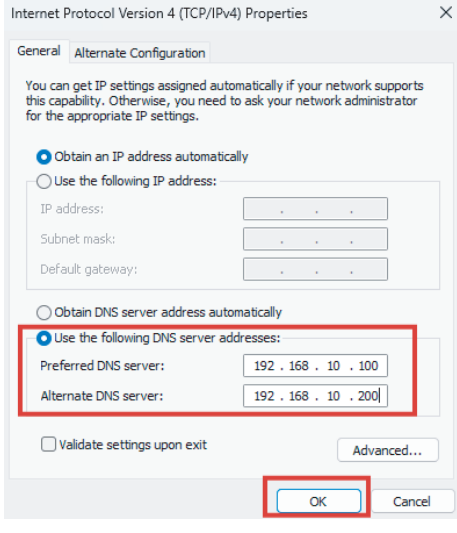
(1) Đối với các thiết bị chạy HĐH Windows:

- Vào Ethernet Properties



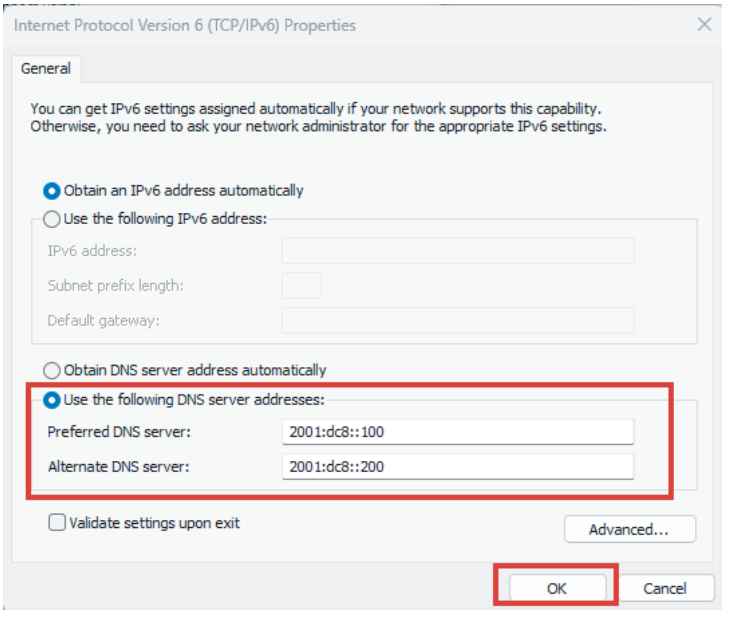
Hình 82: Thiết lập máy chủ phân giải DNS trên HĐH Windows (1)

- Chọn và Internet Protocol Version 4 (TCP/IPv4) -> Properties để thiết lập địa chỉ máy chủ DNS trỏ về máy chủ DNS Caching vừa được thiết lập (đối với IPv4).



Hình 83: Thiết lập máy chủ phân giải DNS trên HĐH Windows (2)

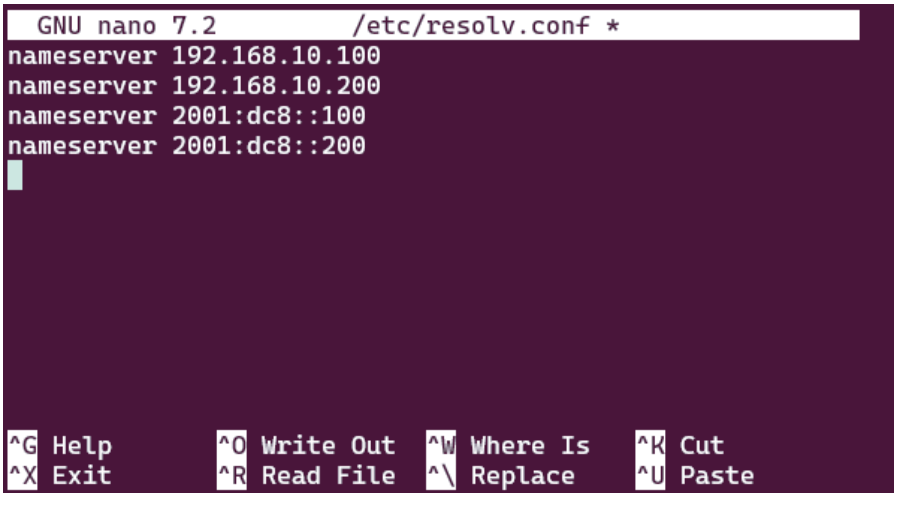
- Tương tự, chọn và Internet Protocol Version 6 (TCP/IPv6) -> Properties để thiết lập địa chỉ máy chủ DNS trỏ về máy chủ DNS Caching vừa được thiết lập (đối với IPv6).



Hình 84: Thiết lập máy chủ phân giải DNS trên HĐH Windows (3)

(2) Đối với các thiết bị chạy HĐH Unix/Linux

Thực hiện thay đổi thông tin máy chủ DNS Caching (DNS resolver) trong file cấu hình /etc/resolv.conf.



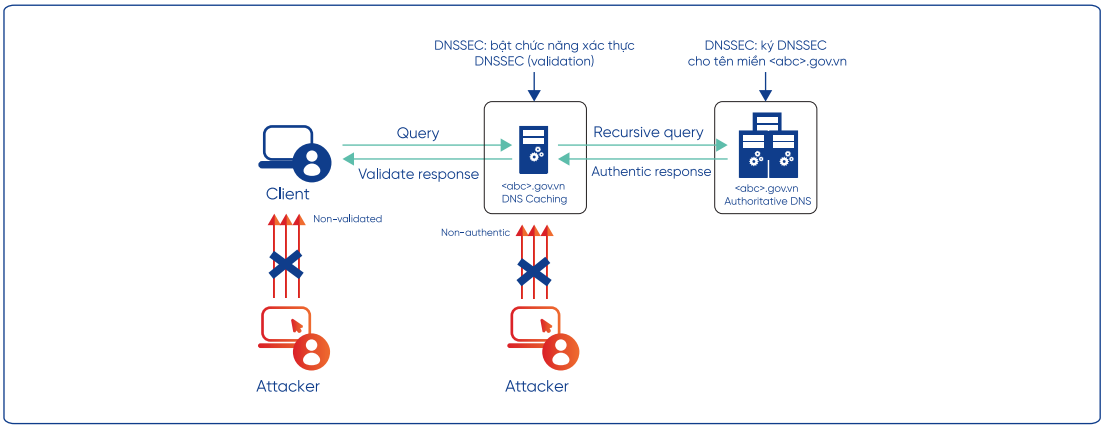
Hình 85: Thiết lập máy chủ phân giải DNS trên HĐH Unix/Linux

2.3. LAB-3: DNSSEC

2.3.1. Phần 1: DNSSEC Validation (xác thực DNSSEC)

Trong nội dung bài lab này, chúng ta sẽ sử dụng phần mềm BIND9 (đã được cài đặt, cấu hình sẵn trong phần thực hành DNS cơ bản).

Mô hình LAB như sau:



Hình 86: Mô hình Lab-3 - Truy vấn xác thực DNSSEC

(1) Cấu hình kích hoạt và xác thực DNSSEC (DNSSEC Validation)

- Cấu hình kích hoạt DNSSEC trên các máy chủ Authoritative DNS Server
- Thực hiện thêm dòng cấu hình: dnssec-enable yes; trong file cấu hình /etc/named.conf

```
#vi /etc/named.conf
options {
   ...
   dnssec-enable yes;
};
```

- Cấu hình kích hoạt và xác thực DNSSEC trên máy chủ DNS Recursive
- Thực hiện thêm dòng cấu hình: dnssec-enable yes; và thêm dòng bật tính năng xác thực DNSSEC vào: dnssec-validation yes; trong file cấu hình /etc/named.conf

```
#vi /etc/named.conf
options {
   ...
   dnssec-enable yes;
   dnssec-validation yes;
};
```

- Một số vấn đề lưu ý đối với tham số dnssec-validation:
+ auto: trust anchor cho DNS Root được tự động sử dụng. Điều này được tích hợp sẵn trong BIND và luôn được cập nhật.
+ yes: trust anchor phải được định cấu hình bằng cách sử dụng câu lệnh "trusted-keys" hoặc "managed-keys".
+ no: tắt tính năng xác thực DNSSEC.

Mặc định thông số dnssec-validation sẽ được thiết lập là "auto".
Trong phần thực hành này chúng ta sẽ thiết lập tham số là "yes", và cấu hình trust anchor.

- Cấu hình Trust Anchor

```
trusted-keys {
                . 257 3 8 "<key-here>";
};
```

+ <key-here>: là chuỗi khóa công khai (DNSKEY) của tên miền Root "."

```
"AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3 +/4RgWOq7HrxRixHlFlEx-
OLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R-
8PzgCmr3EgVLrjyBxWezF 0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd RUfhHdY6+cn8HFRm+2hM8AnXGX-
ws9555KrUB5qihylGa8subX2Nn6UwN R1AkUTV74bU="
```

- Thực hiện thêm cấu hình phần trust anchor trong file cấu hình chung: /etc/named.conf

```
"AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3 +/4RgWOq7HrxRixHlFlEx-
OLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R-
8PzgCmr3EgVLrjyBxWezF 0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd RUfhHdY6+cn8HFRm+2hM8AnXGX-
ws9555KrUB5qihylGa8subX2Nn6UwN R1AkUTV74bU="
```

- Thực hiện thêm cấu hình phần trust anchor trong file cấu hình chung: /etc/named.conf

```
#vi /etc/named.conf
options {
   ...
   dnssec-enable yes;
   dnssec-validation yes;
};
trusted-keys {
                    . 257 3 8 "AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv ArMtNROxVQuCaS-
nIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF 0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/
b58Da+sqqls3eNbuv7pr+e oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd RUfh-
HdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN R1AkUTV74bU="
;
}
```

- Lưu cấu hình và khởi động lại phần mềm BIND và kiểm thử xác thực DNSSEC.

```
#systemctl restart named
```

(2) Kiểm tra hoạt động DNSSEC cho máy chủ DNS Caching

***) Kiểm tra với các kết quả có xác thực**

Chúng ta có thể sử dụng công cụ dòng lệnh DIG để kiểm tra hoạt động xác thực DNSSEC của máy chủ DNS Caching. Mục tiêu là để chứng minh rằng trình xác thực của máy chủ tên miền bộ nhớ đệm (DNS Caching) vừa được triển khai có thể xác thực một cách chính xác các câu trả lời DNS cho các tên miền được ký DNSSEC.

Trong quá trình thử nghiệm, thực hiện truy vấn bản ghi A cho tên miền www.vnnic.vn và kiểm tra bằng cách xác định giá trị cờ (flags) được phản hồi lại.

```
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @8.8.8.8 vnnic.vn A +dnssec +multi
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51339
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;vnnic.vn.          IN A

;; ANSWER SECTION:
vnnic.vn.          17678 IN A 203.119.8.93
vnnic.vn.          17678 IN RRSIG A 8 2 43200 (
                    20250425164421 20250416163921 33906 vnnic.vn.
                    ivvXcM2enc8k+IJygxOqukO+tGh5OHO5TwthgDVO/3u6
                    Xs6MpqEdB+/SOg0z574fSHTlw2fyyxb81cdAIlaFA1up
                    SYvNJy3OTB2lfCXbEMwJZPyYP96hjmlMoju5rcgH0mnR
                    ymkau1YSHsUVix+trkj8635Jia0bjgVtowA9NR8= )
```

Nếu sau khi thực hiện lệnh trên nhận được kết quả với:

- Cờ AD (Authenticated Data) được thiết lập trong quá trình truy vấn DNS/DNSSEC
- Cờ DO (DNSSEC OK) được thiết lập, cho thấy máy chủ DNS Caching có thể nhận thực DNSSEC
- Bản ghi tài nguyên RRSIG được đính kèm trong câu trả lời, với tên miền giống như các bản ghi A.

Đồng nghĩa với việc dữ liệu đã được xác thực với DNSSEC.

***) Kiểm tra với các kết quả KHÔNG có xác thực**

Mục tiêu của kiểm tra này là để chứng minh rằng trình xác thực của máy chủ tên miền bộ nhớ đệm (DNS Caching) sẽ loại bỏ dữ liệu tên miền cùng với chữ ký số.

Trong phần kiểm tra này, thực hiện gửi một truy vấn bản ghi A cho tên miền **dnssec-failed.org** và kiểm tra xem rằng các máy chủ không cung cấp câu trả lời và trả về đúng mã lỗi.

Thực hiện bằng dòng lệnh sau:

```
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @8.8.8.8 dnssec-failed.org A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 43458
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
; EDE: 9 (DNSKEY Missing): (No DNSKEY matches DS RRs of dnssec-failed.org)
;; QUESTION SECTION:
;dnssec-failed.org.          IN     A
```

Dựa vào kết quả trên có thể thấy, không có câu trả lời được cung cấp cho các truy vấn và các máy chủ trả về mã lỗi "SERVFAIL" (phần in đậm màu vàng).

***) Phát hiện lỗi của quá trình xác thực**

Khi nhận được một kết quả với mã lỗi "SERVFAIL" như trường hợp trên, đây cũng có thể là một lỗi liên quan đến trình xác thực. Để kiểm chứng, bằng cách thêm cờ "+cd" (checking disable) để vô hiệu hóa DNSSEC trong lệnh dig.

Nếu khi thêm cờ "+cd" trả về kết quả truy vấn thành công, tiếp tục thực hiện với việc không thêm cờ "+cd", nếu cuối cùng thu được phản hồi "SERVFAIL" đồng nghĩa với trình xác thực gặp vấn đề.

```
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @8.8.8.8 dnssec-failed.org A +cd +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37382
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;dnssec-failed.org.          IN     A

;; ANSWER SECTION:
dnssec-failed.org.     300    IN     A      96.99.227.255
dnssec-failed.org.     300    IN     RRSIG  A 5 2 300 20250428145125 20250411144625 44973 dnssec-failed.
org.  4loh67he6W2XkowzlWs5W9mr7pEhs5WVzKmWpmOfDEF6r77O8Zx+tu5g  uYy6daOoqvKTzEEViCNY-
9GRuobvN+49m+gsv85tCsry7mKKYs2VYyH5H      N+Gt88wexmY7VPMqDYelM51v4l6VkUVWEDrwFCsSxqX-
e58FXCAfn/zxf jPQ=
```

***) Sử dụng công cụ dòng lệnh delv để kiểm chứng**

Đối với các phiên bản BIND từ 9.10 trở lên, có thể sử dụng Domain Entity Lookup & Validation (delv) để thực hiện xác thực các cài đặt. Công cụ này tương tự công cụ dig, nhưng nó được thiết kế đặc biệt cho DNSSEC.

- Nếu xác thực lỗi, do tên miền bị lỗi triển khai DNSSEC, kết quả kiểm tra như sau:

```
# delv @8.8.8.8 dnssec-failed.org A
;; resolution failed: SERVFAIL
```

- Nếu tên miền được triển khai ký và xác thực DNSSEC thành công, kết quả như sau:

```
# delv @8.8.8.8 www.vnnic.vn A
; fully validated
www.vnnic.vn.          19972   IN      A       203.119.8.93
www.vnnic.vn.          19972   IN      RRSIG   A 8 3 43200 20250425164421 20250416163921 33906 vnnic.vn. RUFX-
KDaCSLJKCTG3zAy+a0smbTn1jiGz66RpsEJ+yl+4X0Dno1k22K2p  sRpPBEX6GfoMlQRkia1uFoJMk3lK1tj/Jw-
1bvStNLLxHYXPwKXsnhj7y jXiEgLErbVAOxYQRn3CEplugGhuDuMF7A2CJzd3KYxMWmjwLzCQvTxJJ 2oQ=
```

Nếu sử dụng lệnh trên và thêm vào thông số +rtrace có thể xem được quá trình thực hiện xác thực câu trả lời:

```
# delv @8.8.8.8 www.vnnic.vn A +rtrace +multiline
;; fetch: www.vnnic.vn/A
;; fetch: vnnic.vn/DNSKEY
;; fetch: vnnic.vn/DS
;; fetch: vn/DNSKEY
;; fetch: vn/DS
;; fetch: ./DNSKEY
; fully validated
www.vnnic.vn.          13592 IN A 203.119.8.93
www.vnnic.vn.          13592 IN RRSIG A 8 3 43200 (
                       20250425164421 20250416163921 33906 vnnic.vn.
                       RUFXKDaCSLJKCTG3zAy+a0smbTn1jiGz66RpsEJ+yl+4
                       X0Dno1k22K2psRpPBEX6GfoMlQRkia1uFoJMk3lK1tj/
                       Jw1bvStNLLxHYXPwKXsnhj7yjXiEgLErbVAOxYQRn3CE
                       plugGhuDuMF7A2CJzd3KYxMWmjwLzCQvTxJJ2oQ= )
```

2.3.2. Phần 2: Ký DNSSEC bằng phương pháp thủ công (Manual DNSSEC Signing)

Trong nội dung phần thực hành này, chúng ta sẽ tiến hành thực hiện tạo khóa, ký trên máy chủ Authoritative DNS Server (DNS Primary)

Bước 1: Tạo các cặp khóa (Generate key pairs)

- Tạo đường dẫn chứa các cặp khóa được tạo ra

```
#mkdir -p /etc/named/dnssec/keys
```

- Tạo cặp Khóa ký zone (Zone Singing Keys – ZSK)

```
#cd /etc/named/dnssec/keys
#dnssec-keygen -r /dev/urandom -a rsasha256 -b1024 -n ZONE <ten_mien>.vn
```

- Tạo cặp Khóa ký Khóa (Key Singing Keys – KSK)

```
#dnssec-keygen -r /dev/urandom -a rsasha256 -b2048 -f KSK -n ZONE <ten_mien>.vn
```

Sau khi các cặp khóa được tạo thành công, chúng ta tiến hành chèn các khóa công khai vào trong zone dữ liệu tên miền.

```
#vi /etc/named/<ten_mien>.vn
```

+ Chèn các dòng sau:

```
$INCLUDE "/etc/named/dnssec/keys/K<ten_mien>.vn+008+<zsk_keytag>.key"
$INCLUDE "/etc/named/dnssec/keys/ K<ten_mien>.vn +008+<ksk_keytag>.key"
```

Bước 2: Ký zone

- Lệnh thực hiện ký zone:

```
dnssec-signzone -o <zonename> -N INCREMENT -f <output-file> -t -k <KSKfile> <zonefile>
```

- Trong nội dung bài lab này sẽ thực hiện ký như sau:

```
dnssec-signzone -o <ten_mien>.vn -N INCREMENT -t -k /etc/named/dnssec/keys/K<ten_mien>.
vn.+008+12345 /etc/named/db.<ten_mien>.vn /etc/named/dnssec/keys/K<ten_mien>.vn.+008+12345
```

Sau khi zone đã được ký sẽ xuất hiện có file dữ liệu zone có đuôi là **.signed.** Do đó, với phương pháp ký thủ công, chúng ta phải thực hiện thay đổi cấu hình trỏ tới file dữ liệu zone đã được ký như sau:

```
#vi /etc/named.conf

zone <ten_mien>.vn {
   type master;
   file "/etc/named/db.<ten_mien>.vn.singed";
};
```

- Kiểm tra file cấu hình và khởi động lại BIND

```
#named-checkconf /etc/named.conf
#systemctl restart named
```

- Kiểm tra hoạt động DNSSEC:

```
#dig @localhost <ten_mien>.vn +dnssec
```

2.3.3. Phần 3: Ký tự động (Automatic Signing)

Trong thực tế, phương pháp ký tự động được áp dụng rộng rãi hơn, giúp dễ dàng trong quản trị, vận hành và giảm thiểu các sai sót không đáng có trong ký thủ công.

Bước 1: Cấu hình máy chủ DNS Primary

- Thực hiện tạo khóa: tương tự với Bước 1 trong nội dung Phần 2 với zone tên miền mới:
- Tạo cặp Khóa ký zone (Zone Singing Keys – ZSK)

```
#cd /etc/named/dnssec/keys
#dnssec-keygen -r /dev/urandom -a rsasha256 -b1024 -n ZONE <ten_mien>.vn
```

- Tạo cặp Khóa ký Khóa (Key Singing Keys – KSK)

```
#dnssec-keygen -r /dev/urandom -a rsasha256 -b2048 -f KSK -n ZONE <ten_mien>.vn
```

- Thay đổi nội dung cấu hình trong file cấu hình /etc/named.conf với các thông tin như sau:

```
#vi /etc/named.conf

Zone {
    type master;
    file "/etc/named/db.<ten_mien>.vn;
    auto-dnssec maintain;
    inline-signing yes;
};
```

- Thực hiện kiểm tra file cấu hình và khởi động lại phần mềm BIND để ký DNSSEC:

```
#named-checkconf /etc/named.conf
#systemctl restart named
```

Lưu ý: các thư mục chứa khóa, file cấu hình, file dữ liệu zone tên miền cần được phân quyền cho user/group named:

```
#chown -R named:named /etc/named/
```

- Kiểm tra hoạt động DNSSEC:

```
#dig @localhost <ten_mien>.vn +dnssec
```

2.3.4. Phần 4: Chuỗi tin cậy (Chain of trust)

Bước 1: Tạo bản ghi ký chuyển gia DS – Delegation Signer

Sau khi hoàn tất việc ký các zone tên miền, để DNSSEC cho thể hoạt động xác thực chính xác nguồn gốc tên miền, chúng ta cần cập nhật bản ghi ký chuyển giao DS lên zone tên miền cha "parent zone" để hoàn thành chuỗi xác thực.

- Tạo bản ghi ký chuyển giao DS

```
#dig @localhost dnskey <ten_mien>.vn | dnssec-dsfromkey -f - <ten_mien>.vn > /etc/named/dnssec/
keys/dsset- <ten_mien>.vn
```

Bước 2: Gửi cập nhật bản ghi DS lên Parent zone

- Thông tin bản ghi DS có dạng như sau:

```
<ten_mien>.vn. DS 51646 8 1 A0A6D8C935811B431681EED472652299E750F2DD
<ten_mien>.vn.DS516468280D2C4D8C26C7FE15E4BE468C53B4FA30BCE3B10614A1778A40691C718A30D9B
```

- Kiểm tra, xác thực thông tin bản ghi DS đã cập nhật:

```
#dig @<parent-dns> <ten_mien>.vn DS +multiline
```

2.3.5. Phần 5: DNSSEC Key Rollover

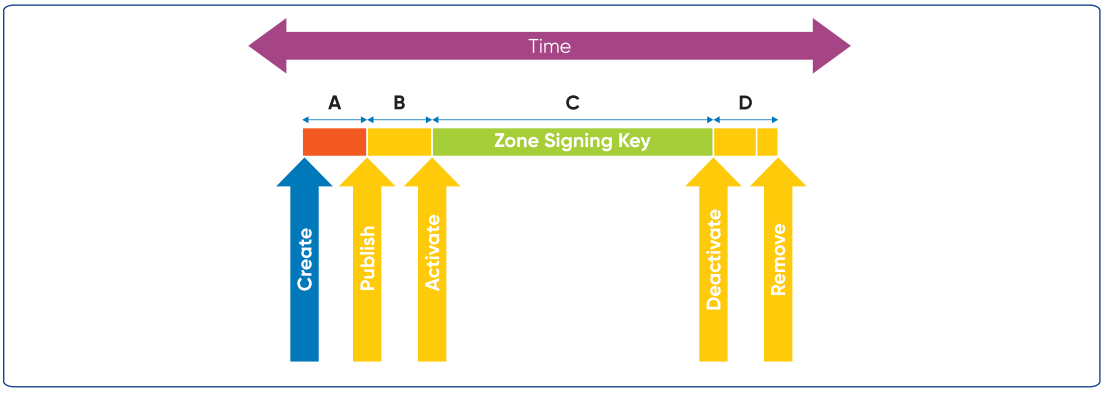
Thực hiện thay khóa DNSSEC bao gồm thay thế các khóa KSK và ZSK.

Trong thực tế, thông thường các khóa KSK và ZSK được thay khóa như sau:

- KSK sẽ được thay khóa sử dụng phương pháp Double-Signing, và chu kỳ thay khóa khuyến nghị từ 1-3 năm.
- ZSK sẽ được thay khóa sử dụng phương pháp Pre-Public, chu kỳ thay khóa khuyến nghị từ 3-6 tháng 1 lần.

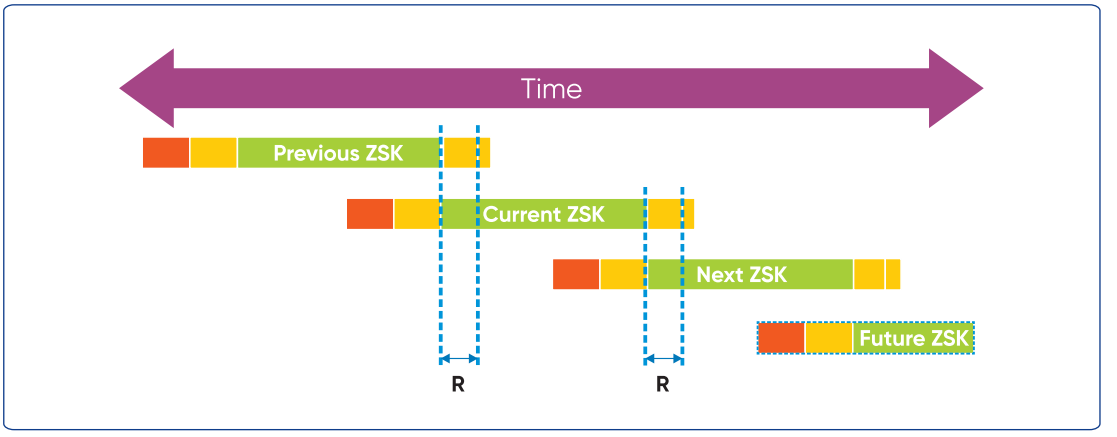
Trước khi đi vào thực hiện các bước chi tiết, chúng ta cần hiểu rõ các tham số sau của mỗi loại khóa:

+ Create: thời điểm khóa được khởi tạo
+ Published: thời điểm khóa được công khai, nhưng chưa được sử dụng để ký.
+ Activate: thời điểm khóa được công khai và ký cho các bản ghi DNS.
+ Deactive: thời điểm mà khóa không còn được ký cho các bản ghi DNS, tuy nhiên khóa này vẫn đang được công khai.
+ Remove: thời điểm khóa được xóa và không còn được sử dụng.



Hình 87: Các mốc thời gian trong quá trình thay khóa DNSSEC

Bước 1: ZSK Rollver với phương pháp pre-public



Hình 88: Timeline quá trình thay khóa DNSSEC với pre-public

- Thực hiện tạo khóa mới:

```
dnssec-keygen -r /dev/urandom <ten_mien>.vn
```

- Kiểm tra nội dung khóa vừa tạo:

```
#more K<ten_mien>.vn.+008+56789.key
```

Lưu ý các thông số, đặc biệt là thời gian Public và thời gian Active, các thời gian này mặc định khi tạo chính là thời điểm tạo khóa (Create)

```
; This is a zone-signing key, keyid 1335, for irrashai.net
; Created: 20220220130716 (Mon Feb 20 13:07:06 2022)
; Publish: 20220220130716 (Mon Feb 20 13:07:06 2022)
; Activate: 20220220130716 (Mon Feb 20 13:07:06 2022)
```

- Thiết lập các tham số thời gian cho khóa ZSK cũ và mới:

```
#cd /etc/named/dnssec/keys
dnssec-settime -I 20220322 -D 20220622 K<ten_mien>.vn.+008+12345
```

+ Tham số -I là thời điểm khóa sẽ hết hạn (Inactive)
+ Tham số -D là thời điểm khóa sẽ bị xóa
- Thiết lập tham số thời gian cho khóa vừa tạo:

```
#cd /etc/named/dnssec/keys
dnssec-settime -P 20220320 -I 20220422 K<ten_mien>.vn.+008+12345
```

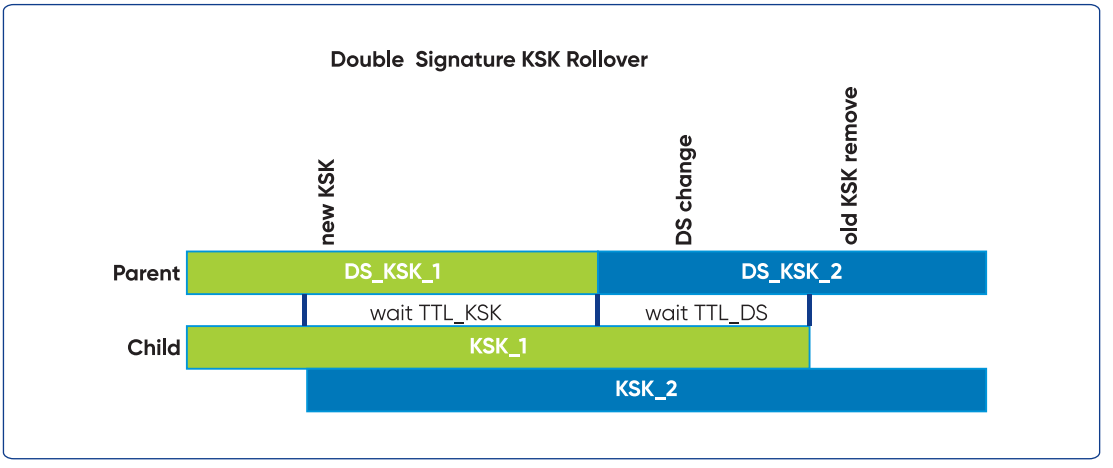
- Khởi động lại phần mềm BIND để áp dụng thay khóa ZSK:

```
#systemctl restart named
```

- Kiểm tra hoạt động DNSSEC với khóa mới đã được thay

```
#dig @localhost <ten_mien>.vn DNSKEY +dnssec +multiline
```

Bước 2: Thực hiện thay khóa KSK với phương pháp Double-Signing



Hình 89: Timeline quá trình thay khóa DNSSEC với double-signature

Đối với khóa KSK, để đảm bảo an toàn, chúng ta sẽ thực hiện thay khóa bằng phương pháp Double-Signing, tức là sử dụng 02 cặp khóa KSK mới và cũ để ký. Sau đó sẽ thiết lập lại tham số thời gian, thay thế khóa cũ hoàn toàn bằng khóa mới.

- Tạo khóa KSK mới:

```
#dnssec-keygen -r /dev/urandom -a rsasha256 -b2048 -f KSK -n ZONE <ten_mien>.vn
```

- Thực hiện khởi động lại phần mềm BIND để tiến hành ký:

```
#systemctl restart named
```

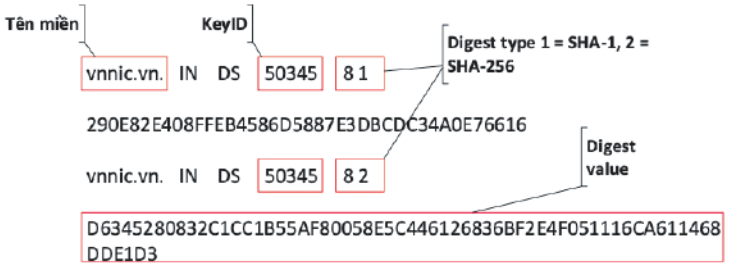
- Cập nhật bản ghi ký chuyển gia (DS – Delegation Signer) mới lên "Parent zone"

+ Cách tạo bản ghi DS:

```
#dig @localhost DNSKEY <ten_mien>.vn | dnssec-dsfromkey -f – <ten_mien>.vn > /etc/named/dnssec/
keys/dsset-<ten_mien>.vn
```

+ Sau khi bản ghi DS được tạo ra sẽ lưu tại: /etc/named/dnssec/keys/dsset-<ten_mien>.vn

Bản ghi DS sẽ có định dạng như sau:



Hình 90: Định dạng bản ghi ký chuyển giao DS – Delegation Signer

+ Sử dụng thông tin bản ghi DS và gửi cập nhật lên hệ thống quản lý "parent zone", trong trường hợp này, parent zone của <ten_mien>.vn là .vn. Do đó, cần cập nhật các bản ghi DS vào zone tên miền .VN thông qua hệ thống Portal của Nhà đăng ký tên miền và sẽ được cập nhật vào cơ sở dữ liệu của hệ thống tên miền (DNS) quốc gia.
+ Sau khi cập nhật bản ghi DS mới thành công, chúng ta tiến hành thiết lập tham số thời gian của khóa KSK cũ và mới:

Ví dụ:

- Khóa cũ sẽ hết hiệu lực sau 01 tháng và sẽ xóa sau 04 tháng tính tại thời điểm Rollover Key.
- Khóa mới sẽ thiết lập các thông số mặc định (có hiệu lực vô thời hạn, và có hiệu lực ngay tại thời điểm tạo khóa)

```
#cd /etc/named/dnssec/keys
dnssec-settime -I 20250522 -D 20250822 K<ten_mien>.vn.+008+22222
```

+ Ngay sau khi khóa cũ hết hiệu lực (tức tại thời điểm Inactive), chúng ta tiến hành thực hiện yêu cầu xóa bản ghi DS tương ứng với khóa cũ của tên miền thông qua Portal của Nhà đăng ký tên miền.

Bước 3: Kiểm tra hoạt động DNSSEC

Có thể sử dụng một số công cụ phổ biến dưới đây để kiểm tra và đảm bảo hệ thống DNSSEC hoạt động ổn định.

(1) WHOIS

Tiến hành kiểm tra trên công cụ Whois của VNNIC nhằm đảm bảo việc bản ghi DS của tên miền đã được cập nhật thành công lên hệ thống quản lý, cấp phát tên miền quốc gia .VN như kết quả minh họa dưới đây:

Kết quả tra cứu thông tin tên miền

Tên miền:	godns.vn
Tên chủ thể đăng ký sử dụng:	NGUYỄN VĂN TRÍ
Nhà đăng ký quản lý:	Công ty TNHH P.A Việt Nam
Ngày đăng ký:	2024-01-03
Ngày hết hạn:	2026-01-03
Trạng thái:	clientTransferProhibited
Máy chủ DNS chuyển giao:	ns1.godns.vn ns2.godns.vn
DNSSEC:	Đã ký chuyển giao

Hình 91: Hình minh họa tra cứu WHOIS

(*) Nếu trạng thái DNSSEC là "Đã ký chuyển giao" tức là các bản ghi DS đã được cập nhật thành công

(2) dig hoặc nslookup

Sử dụng công cụ dig hoặc nslookup để kiểm tra thông tin các bản ghi DS trên hệ thống máy chủ tên miền (DNS) quốc gia và kiểm tra truy vấn xác thực DNSSEC.

- Truy vấn bản ghi DS:

```
$ dig @b.dns-servers.vn. godns.vn DS +norec

; <<>> DiG 9.10.1 <<>> godns.vn. DS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49949
;; flags: qr aa ; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;godns.vn.                              IN          DS

;; ANSWER SECTION:
godns.vn.  61179     IN          DS          28267 8 1 66D47CE4B4F551BE5EDA43AC5F3109E8C98E2FAE
godns.vn.  61179     IN          DS          28267     8     2     71D9335416B7132519190A95685E18CBF478DCF-
4CA98867062777938F8FEAB89
```

(**) Kết quả trong phần ANSWER SECTION cho thấy các bản ghi DS đã được cập nhật và truy vấn thành công trên DNS quốc gia.

- Truy vấn xác thực DNSSEC:

Để thực hiện truy vấn xác thực DNSSEC, chúng ta cần thực hiện truy vấn đến máy chủ DNS resolver (DNS Caching) đã bật xác thực DNSSEC (như DNS Caching của VNNIC, Google Public DNS, Cloudflare DNS,...).

```
# dig @192.168.10.100 www.godns.vn. A +dnssec +multiline

; <<>> DiG 9.10.0-P2 <<>> @192.168.1.7 www.godns.vn. A +dnssec +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32472
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.godns.vn.                  IN A

;; ANSWER SECTION:
www.godns.vn.                  4 IN A       149.20.64.69
www.godns.vn.                  4 IN RRSIG A 5 3 60 (
                                            20141029233238 20140929233238 4521 godns.vn.
                                            DX5BaGVd4KzU2AIH911Kar/UmdmkARyPhJVLr0oyPZaq
                5zoobGqFl4efvzL0mcpncuUg3BSU5Q48WdBu92xinMdb
                E75zl+adgEBOsFgFQR/zqM3myt/8SngWm4+TQ3XFh9eN
                jqExHZZuZ268NtlxqgF9OmKRRv8X8YigaPShuyU= )
```

Nếu sau khi thực hiện lệnh trên nhận được kết quả với:

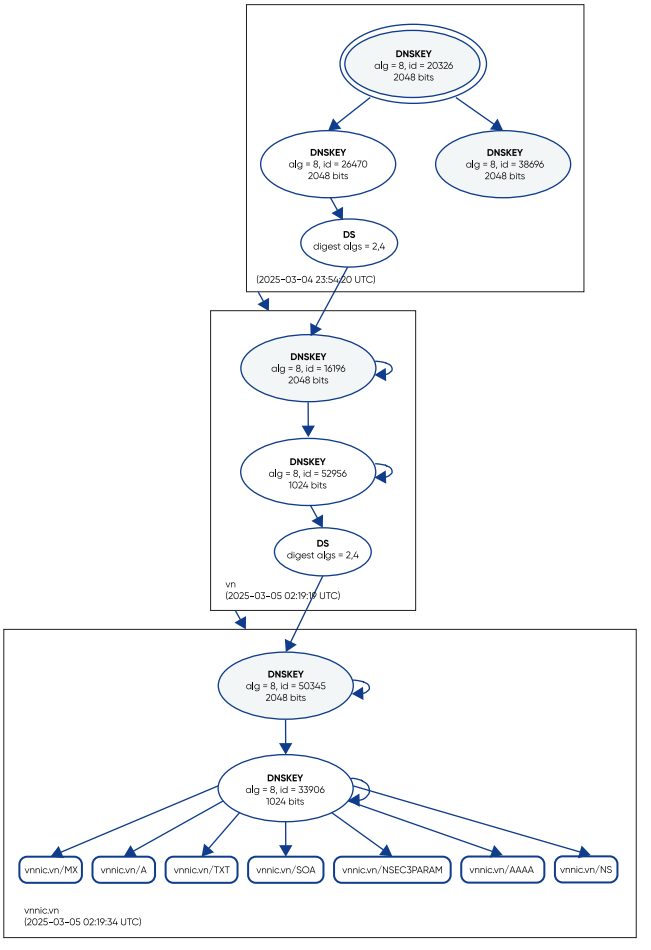
- Cờ AD (Authenticated Data) được thiết lập trong quá trình truy vấn DNS/DNSSEC
- Cờ DO (DNSSEC OK) được thiết lập, cho thấy máy chủ DNS Caching có thể nhận thực DNSSEC
- Bản ghi tài nguyên RRSIG được đính kèm trong câu trả lời, với tên miền giống như các bản ghi A.

Đồng nghĩa với việc dữ liệu đã được xác thực với DNSSEC thành công.

(3) Sử dụng các công cụ Online

Cách sử dụng các công cụ đã được mô tả chi tiết trong mục X **"Các công cụ hỗ trợ quản lý, vận hành"** phần I của cuốn sách.

Dưới đây là ví dụ về sử dụng công cụ phổ biến cho DNSSEC:



Hình 92: Kết quả kiểm tra DNSSEC bằng công cụ DNSviz

TÀI LIỆU THAM KHẢO

1. Sách tham khảo

[1] Cricket Liu. DNS & BIND Cookbook. O'Reilly Media, Inc, 2002.
[2] Ron Aitchison. Pro DNS and BIND 10. Apress, 2005.
[3] Cricket Liu. DNS & BIND on IPv6. O'Reilly Media, Inc, 2011.
[4] Joshua M Kuo, Ross Gibson J.D. The Hidden Potential of DNS In Security: Combating Malware, Data Exfiltration, and more - The Guide for Security Professionals. Infoblox, 2023.
[5] Hoàng Minh Cường, Phạm Việt Anh. Hướng dẫn cài đặt máy chủ DNS. Nhà xuất bản Bưu điện, 2006.

2. Danh sách các RFC chính

SỐ RFC	TIÊU ĐỀ	MÔ TẢ
RFC 1034	Domain names - concepts and facilities	Cung cấp các khái niệm và cơ sở về hệ thống tên miền, bao gồm cấu trúc tên miền, phân cấp và các khái niệm cơ bản khác.
RFC 1035	Domain names - implementation and specification	Định nghĩa chi tiết về cách triển khai và đặc tả của hệ thống tên miền, bao gồm các loại bản ghi và cách thức hoạt động của DNS.
RFC 1183	New DNS RR Definitions	Đưa ra các định nghĩa mới cho các bản ghi tài nguyên (RR) trong DNS, mở rộng khả năng của hệ thống tên miền.
RFC 1591	Domain Name System Structure and Delegation	Mô tả cấu trúc và phân quyền trong hệ thống tên miền, bao gồm cách thức phân quyền và quản lý các miền cấp cao.
RFC 1794	DNS Support for Load Balancing	Cung cấp thông tin về cách DNS hỗ trợ cân bằng tải, bao gồm các phương pháp và kỹ thuật liên quan.
RFC 1912	Common DNS Operational and Configuration Errors	Liệt kê các lỗi cấu hình và vận hành phổ biến trong DNS, cung cấp hướng dẫn để tránh và khắc phục chúng.
RFC 1982	Serial Number Arithmetic	Mô tả cách thức tính toán số serial trong DNS, đảm bảo tính nhất quán và đồng bộ của các bản sao zone tên miền.
RFC 1995	Incremental Zone Transfer in DNS	Đề xuất phương pháp đồng bộ dữ liệu zone trong DNS, giúp giảm thiểu băng thông và thời gian khi cập nhật dữ liệu.
RFC 1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)	Cung cấp cơ chế thông báo kịp thời về các thay đổi trong zone DNS, hỗ trợ việc đồng bộ hóa nhanh chóng giữa các máy chủ.
RFC 2136	Dynamic Updates in the Domain Name System (DNS UPDATE)	Định nghĩa cách thức cập nhật động trong hệ thống tên miền, cho phép thay đổi dữ liệu DNS mà không cần khởi động lại máy chủ.
RFC 2181	Clarifications to the DNS Specification	Cung cấp các làm rõ và sửa đổi đối với các đặc tả DNS, giúp cải thiện tính chính xác và hiệu quả của hệ thống.
RFC 2230	Key Exchange Delegation Record for the DNS	Định nghĩa bản ghi ủy quyền trao đổi khóa trong DNS, hỗ trợ việc quản lý và phân phối khóa an toàn.

SỐ RFC	TIÊU ĐỀ	MÔ TẢ
RFC 2308	Negative Caching of DNS Queries (DNS NCACHE)	Đề xuất phương pháp lưu trữ kết quả truy vấn DNS không thành công, giúp giảm tải cho máy chủ và cải thiện hiệu suất.
RFC 2317	Classless IN-ADDR.ARPA delegation	Định nghĩa phương pháp chuyển giao tên miền ngược (reverse delegation) không theo lớp trong IN-ADDR.ARPA, hỗ trợ việc phân giải tên miền ngược cho các địa chỉ IP không theo lớp truyền thống.
RFC 2535	Domain Name System Security Extensions (DNSSEC)	Mở rộng hệ thống tên miền với các tính năng bảo mật, bao gồm xác thực và toàn vẹn dữ liệu.
RFC 2671	Extension Mechanisms for DNS (EDNS0)	Cung cấp cơ chế mở rộng cho DNS, cho phép truyền tải các thông tin bổ sung trong các truy vấn và phản hồi.
RFC 2782	A DNS RR for specifying the location of services (DNS SRV)	Định nghĩa bản ghi DNS SRV, cho phép xác định vị trí của các dịch vụ trong mạng.
RFC 2845	Secret Key Transaction Authentication for DNS (TSIG)	Cung cấp cơ chế xác thực dựa trên khóa bí mật cho các giao dịch DNS, đảm bảo tính toàn vẹn và bảo mật.
RFC 2930	DNS Support for IP Multicast	Mô tả cách DNS hỗ trợ địa chỉ đa hướng IP, bao gồm các bản ghi và phương pháp liên quan.
RFC 3225	DNS Security Operational Practices (DNSOP)	Cung cấp các thực hành vận hành bảo mật cho DNS, bao gồm cấu hình và quản lý an toàn.
RFC 3363	DNS Security Threats and Countermeasures	Mô tả các mối đe dọa bảo mật đối với DNS và các biện pháp đối phó tương ứng.
RFC 4033	DNS Security Introduction and Requirements	Giới thiệu và các yêu cầu bảo mật DNS: Định nghĩa mục tiêu và yêu cầu cho DNSSEC.
RFC 4034	Resource Records for the DNS Security Extensions	Định nghĩa các bản ghi tài nguyên cho các mở rộng bảo mật DNS (DNSSEC), bao gồm các bản ghi như DNSKEY, DS, RRSIG và NSEC.
RFC 4035	Protocol Modifications for the DNS Security Extensions	Cung cấp các sửa đổi giao thức cho các mở rộng bảo mật DNS (DNSSEC), bao gồm các thay đổi cần thiết để hỗ trợ tính năng bảo mật.
RFC 5155	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence	Mô tả việc sử dụng NSEC3, một phương pháp mới để cải thiện bảo mật và quyền riêng tư trong DNSSEC bằng cách che giấu cấu trúc zone DNS.
RFC 5702	Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC	Mô tả việc sử dụng các thuật toán SHA-2 với RSA trong các bản ghi tài nguyên DNSKEY và RRSIG, nhằm cải thiện độ bảo mật của DNSSEC.
RFC 6672	DNAME Redirection in the DNS	Định nghĩa việc chuyển hướng tên miền trong DNS bằng cách sử dụng bản ghi DNAME, hỗ trợ việc quản lý và phân giải tên miền hiệu quả hơn.

SỐ RFC	TIÊU ĐỀ	MÔ TẢ
RFC 6686	Resolution of the Sender Policy Framework (SPF) and Sender ID Experiments	Cung cấp thông tin về việc giải quyết các thí nghiệm của Sender Policy Framework (SPF) và Sender ID, hỗ trợ việc xác thực email.
RFC 6698	The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA	Định nghĩa giao thức TLSA trong DANE, hỗ trợ việc xác thực các thực thể có tên trong DNS thông qua TLS.
RFC 6724	Default Address Selection for Internet	Đề xuất các phương pháp chọn lựa địa chỉ mặc định cho giao thức IPv6, hỗ trợ việc quản lý và phân giải địa chỉ hiệu quả hơn.
RFC 6840	Clarifications and Implementation Notes for DNS Security (DNSSEC)	"Cung cấp các làm rõ và ghi chú triển khai cho DNSSEC, nhằm đảm bảo hiểu biết và áp dụng đồng nhất của các tiêu chuẩn."
RFC 6891	Extension Mechanisms for DNS (EDNS(0))	Cung cấp cơ chế mở rộng cho DNS, cho phép truyền tải các thông tin bổ sung trong các truy vấn và phản hồi, hỗ trợ các tính năng mới như DNSSEC và DNS-over-HTTPS.
RFC 6895	Domain Name System (DNS) IANA Considerations	Đề xuất các xem xét về IANA đối với DNS, bao gồm các vấn đề liên quan đến việc quản lý và phân phối tài nguyên DNS.
RFC 6912	Principles for Unicode Code Point Inclusion in Labels in the DNS	Định nghĩa các nguyên tắc cho việc bao gồm các điểm mã Unicode trong nhãn DNS, hỗ trợ việc sử dụng tên miền quốc tế hóa.
RFC 6927	Variants in Second-Level Names Registered in Top-Level Domains	Cung cấp thông tin về các biến thể trong tên miền cấp hai đã đăng ký trong các tên miền cấp cao, hỗ trợ việc quản lý và phân giải tên miền hiệu quả hơn.
RFC 6944	Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status	Cung cấp thông tin về tình trạng triển khai thuật toán DNSKEY trong DNSSEC, hỗ trợ việc xác thực và bảo mật dữ liệu.
RFC 6950	Architectural Considerations on Application Features in the DNS	Đề xuất các xem xét kiến trúc về các tính năng ứng dụng trong DNS, hỗ trợ việc mở rộng và linh hoạt trong việc sử dụng DNS.
RFC 6975	Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC)	Cung cấp thông tin về việc tín hiệu hiểu biết thuật toán mật mã trong các mở rộng bảo mật DNS (DNSSEC), hỗ trợ việc xác thực và bảo mật dữ liệu.
RFC 7583	DNS Security (DNSSEC) and Cookies	Giới thiệu việc sử dụng 'cookies' trong DNSSEC để giảm thiểu các rủi ro liên quan đến tấn công làm lũy tiến.
RFC 7858	Specification for DNS over Transport Layer Security (TLS)	Mô tả việc sử dụng TLS để bảo mật truy vấn DNS, cung cấp tính bảo mật và quyền riêng tư tăng cường cho truy vấn DNS.
RFC 8014	Automating DNSSEC Delegation Trust Maintenance	Mô tả các phương pháp tự động hóa để duy trì tin cậy ủy quyền trong DNSSEC, nhằm cải thiện tính bảo mật và dễ dàng quản lý hơn.

SỐ RFC	TIÊU ĐỀ	MÔ TẢ
RFC 8310	Usage Profiles for DNS over TLS and DNS over DTLS	Hồ sơ sử dụng DoT/DoDTLS – Xác định cách thiết lập kết nối bảo mật giữa client và server
RFC 8484	DNS Queries over HTTPS (DoH)	Mô tả giao thức thực hiện truy vấn DNS qua HTTPS để cải thiện quyền riêng tư và an toàn an ninh.
RFC 9250	Oblivious DNS over HTTPS (ODoH)	Mô tả giao thức DNS mới cho phép truy vấn DNS được thực hiện mà không để lộ danh tính người dùng cho các máy chủ DNS, nhằm tăng cường quyền riêng tư.

VNNIC
Internet for all

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM INTERNET VIỆT NAM

.VN

TÊN MIỀN QUỐC GIA VIỆT NAM

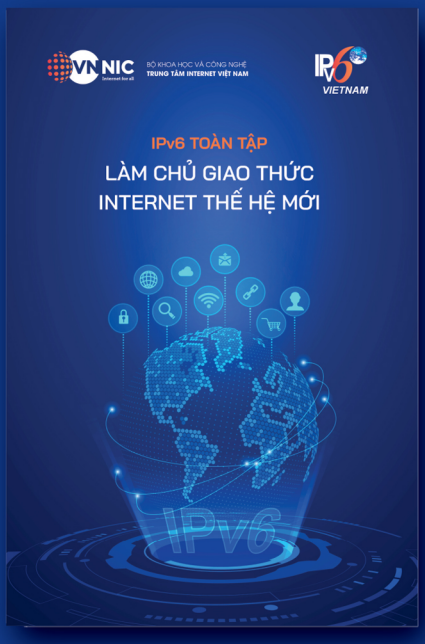
HIỆN DIỆN TRỰC TUYẾN TỰ HÀO VIỆT NAM

.vn | .biz.vn | .pro.vn | hanoi.vn | com.vn | net.vn
edu.vn | gov.vn | org.vn | info.vn | ai.vn | io.vn
name.vn | ac.vn | int.vn | health.vn

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM INTERNET VIỆT NAM

MỘT SỐ CUỐN SÁCH TIÊU BIỂU KHÁC VỀ INTERNET VIỆT NAM

BÁO CÁO INTERNET, TÀI NGUYÊN INTERNET VIỆT NAM 2024



IPv6 TOÀN TẬP LÀM CHỦ GIAO THỨC INTERNET THẾ HỆ MỚI

TRỤ SỞ TẠI TP. HÀ NỘI

• Trụ sở chính: Tòa nhà VNTA, đường Dương Đình Nghệ, P. Yên Hòa, Q. Cầu Giấy, Hà Nội
• Khu công nghệ cao Hòa Lạc, Thạch Thất, Hà Nội
Tel: 024 3556 4944 | Email: info@vnnic.vn | Website: https://vnnic.vn

CHI NHÁNH TẠI TP. ĐÀ NẴNG

Lô 21, Đường số 7, KCN An Đồn, Q. Sơn Trà, TP. Đà Nẵng

CHI NHÁNH TẠI TP. HỒ CHÍ MINH

Đường số 20 - Khu chế xuất Tân Thuận, Q. 7, TP. Hồ Chí Minh

SÁCH KHÔNG BÁN